AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXXIX, Number 4
OCTOBER, 1957

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

CONTENTS

The AMERICAN JOURNAL OF MATHEMATICS appears four times yearly.

The subscription price of the JOURNAL is \$8.50 in the U. S.; \$8.75 in Canada; and \$9.00 in other foreign countries. The price of single numbers is \$2.50.

Manuscipts intended for publication in the JOURNAL should be sent to Professor AUREL WINTNER, The Johns Hopkins University, Baltimore 18, Md.

Subscriptions to the JOURNAL and all business communications should be sent to THE JOHNS HOPKINS PRESS, BALTIMORE 18, MARYLAND, U. S. A.

THE JOHNS HOPKINS PRESS supplies to the authors 100 free reprints of every article appearing in the AMERICAN JOURNAL OF MATHEMATICS. On the other hand, neither THE JOHNS HOPKINS PRESS nor the AMERICAN JOURNAL OF MATHEMATICS can accept orders for additional reprints. Authors interested in securing more than 100 reprints are advised to make arrangements directly with the printers, J. H. FURST CO., 20 HOPKINS PLACE, BALTIMORE 1, MARYLAND.

The typescripts submitted can be in English, French, German or Italian and should be prepared in accordance with the instructions listed on the inside back cover of this issue.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

A CHARACTERISTIC RELATION IN FIBRE BUNDLES.*[1]

By Alfred Adler.

A problem posed by S. S. Chern can be stated as follows: Given a fibre bundle (M, X, F, G, p), whose base space X and bundle space M are Riemannian manifolds, and whose fibre is a homogeneous space of G, what are the Pontrjagin characteristic classes of M in terms of those of X and F? If F is of the form G/K, G a compact Lie group and K a closed connected subgroup of G, an answer is given by Theorem 2.

This paper consists of two parts. In the first, the object is to find the curvature form of M in terms of those of X and F; the result (for the frame bundles) is the content of Theorem 1. In the second part, this curvature form is inserted in the Pontrjagin polynomials of M, which then split into tensor products, giving Theorem 2.

The numbers [1], [2], [3] refer to the bibliography.

Frame bundles. Let (M, X, F, G, p) be a fibre bundle, X and M Riemannian manifolds, G a compact Lie group, and $F = G/K$, K a closed subgroup of G. $B(X)$, $B(F)$, $B(M)$ will denote the bundle spaces of the frame bundles of X, F, M (with respect to Riemannian metrics which will be defined in the next paragraphs); and $O(X)$, $O(F)$, $O(M)$ will denote the orthogonal groups which are the fibres of these bundles. N and n will denote, respectively, the dimensions of X and F.

The definitions of connections and curvature forms can be found in [1].

Let (M', X, G, G, p') be the associated principal bundle of (M, X, F, G, p), and let P be the natural (fibre-preserving) mapping of M' onto M. Note that (M', M, K, K, P) is a fibre bundle. If ϕ is a strip map of the bundle (M, X, F, G, p), we denote the associated strip map of the bundle (M', X, G, G, p') by ϕ'.

We first define a Riemannian metric on M'. Let $(\ ,\ )_G$ be the metric on G given by the fundamental bilinear form (Killing form), and let $(\ ,\ )_X$ be a Riemannian metric on X. Let H_0 be a connection (concept of horizon-

* Received March 20, 1957.

[1] Written under DA 36-034-ORD-2164.

tality) in M' with respect to the bundle (M', X, G, G, p'), and define the metric $(\ ,\ )_{M'}$ on M' in the following way:

(a) if t, t' are vectors at a point m' of M', with $p'm' = x$ and $pt = p't' = 0$, let $(t, t')_{M'} = (\phi_x'^{-1}t, \phi_x'^{-1}t')_B$; this is independent of the strip map ϕ', since the metric on G is invariant;

(b) if t, t' are H_0-horizontal in M', let $(t, t')_{M'} = (p't, p't')_X$;

(c) extend this inner product bilinearly.

Now we define a Riemannian metric on M: Since P is fibre-preserving, a connection H_1 can be defined on M by the condition $H_1 \circ P = P \circ H_0$. Then we define $(\ ,\ )_M$ in terms of the metrics of X and F (the metric of F being that induced by the fundamental bilinear form on G), in the same manner as $(\ ,\ )_{M'}$ was defined in terms of the metrics of X and G.

Reduction of $B(F)$. Let $X_1, \cdots, X_n$ be horizontal orthonormal left-invariant vector fields on G. (By this, we mean horizontal with respect to the following connection ω_F on G: Let $\mathfrak{g}$ be the Lie algebra of G, $\mathfrak{k}$ the Lie algebra of K, and $\mathfrak{m}$ the orthogonal complement of $\mathfrak{k}$ in $\mathfrak{g}$ with respect to the fundamental bilinear form. Then $\mathfrak{g} = \mathfrak{k} + \mathfrak{m}$. If t is a vector of G, we define $\omega_F(t)$ to be the $\mathfrak{k}$-component of the element of $\mathfrak{g}$ resulting from left-translation of t to all points of G.) Let δ be the natural projection of G onto G/K, and let $A_i(gK) = \delta(X_i(g))$ (so A_i depends on g, not only on gK). Let $\bar{\mathfrak{m}} = (eK, A_1(eK), \cdots, A_n(eK))$, and define a mapping Δ of G into $B(F)$ by: $\Delta(g) = (gK, A_1(gK), \cdots, A_n(gK))$. Since $\delta \circ L_g = L_g \circ \Delta$, it follows that $\Delta(g) = L_g(\bar{\mathfrak{m}})$. In particular, if $k \in K$, then $\Delta(k) = L_k(\bar{\mathfrak{m}})$ = the matrix of $\operatorname{ad} k$ with respect to the elements $X_1(e), \cdots, X_n(e)$ of $\mathfrak{g}$, i.e., with respect to a basis of $\mathfrak{m}$. Let $\Delta(g)\Delta(g') = \Delta(gg')$, and define right- and left-translations $R_{\Delta(g)}$ and $L_{\Delta(g)}$ on $\Delta(G)$ in the natural way. Then the bundle $(B(F), F, O(F), O(F), p_F)$ is reducible to the bundle $(\Delta(G), F, \Delta(K), \Delta(K), p_F)$, p_F the natural projection of $B(F)$ onto F.

The connection ω_F on the bundle (G, F, K, K, δ) gives rise to a connection on the bundle $(\Delta(G), F, \Delta(K), \Delta(K), p_F)$, denoted by $\operatorname{ad} \omega_F$. Let Ω_F and $\operatorname{ad} \Omega_F$ denote the curvature forms respectively of ω_F and $\operatorname{ad} \omega_F$. Then for any pair of tangent vectors t, t' at a given point of G, we have:

$$(\operatorname{ad} \Omega_F)(\Delta(t), \Delta(t')) = \operatorname{ad}(\Omega_F(t, t'))[\mathfrak{m}],$$

the symbol on the right side of the equality representing the matrix of $\Omega_F(t, t')$ with respect to the basis $X_1(e), \cdots, X_n(e)$ of $\mathfrak{m}$. $\operatorname{ad} \omega_F$ is the *canonical connection of the* 2^{nd} *kind.*

Reduction of $B(M)$. Let matrix addition be defined by

$$(a_{ij}) \oplus (b_{ij}) = \left(\begin{array}{c|c} a_{ij} & 0 \\ \hline 0 & b_{ij} \end{array}\right).$$

Then the bundle $(B, M, O(X) \oplus \Delta(K), O(X) \oplus \Delta(K), p_M)$ is defined in the following way:

(1) $B = [(m, e_1, \cdots, e_N, f_1, \cdots, f_n) \mid$ the e_i are 'horizontal' vectors at m (with respect to the M-metric), and the f_i are vectors of the form $\phi_x A_i(f)$—where $m = \phi(x, f)$, and ϕ is some strip map of the bundle (M, X, F, G, p).$]$

(2) p_M is the natural projection of B onto M.

(3) The strip maps ϕ^M are defined as follows: Let $\mathfrak{a}_i, i = 1, \cdots, N$, be orthonormal vector fields on a submanifold θ^X of X, and let $\mathfrak{b}_i$, $i = 1, \cdots, n$, be orthonormal vector fields on a submanifold θ^F of F; let ϕ be a strip map of the bundle (M, X, F, G, p). Let $\mathfrak{a}_i'$, $\mathfrak{b}_i'$ be the following vector fields on $\phi(\theta^X, \theta^F)$: $\mathfrak{a}_i'(\phi(x, f)) = \phi(\mathfrak{a}_i(x), 0(f))$, where $0(f)$ is the zero-vector at f; and $\mathfrak{b}_i'(\phi(x, f)) = \phi_x \mathfrak{b}_i(f)$. If the $\mathfrak{b}_i$ are chosen to be the A_i defined previously, and if we let $\phi^M(\phi(x, f), r \oplus \Delta)$ equal

$$(m, \Sigma r_{i1} \mathfrak{a}_i'(m), \cdots, \Sigma r_{iN} \mathfrak{a}_i'(m), \Sigma \Delta_{i1} \mathfrak{b}_i'(m), \cdots, \Sigma \Delta_{in} \mathfrak{b}_i'(M))$$

—$\phi(x, f) = m$, $r \oplus \Delta \in O(X) \oplus \Delta(K)$—then ϕ^M is a strip may of the bundle $(B(M), M, O(M), O(M), p_M)$, and also of the bundle just defined. It follows from the definition of the strip maps of $(B(M), M, O(M), O(M), p_M)$, that this bundle is reducible to the bundle $(B, M, O(X) \oplus \Delta(K) \oplus \Delta(K), p_M)$.

The bundles $(B(X), X, O(X), O(X), p_X)$, $(\Delta(G), F, \Delta(K), \Delta(K), p_X)$, and $(B, M, O(X) \oplus \Delta(K), O(X) \oplus \Delta(K), p_M)$ will be denoted respectively by $\mathfrak{B}(X)$, $\mathfrak{B}(F)$, and $\mathfrak{B}(M)$.

$(B, B(X), \Delta(G), \Delta(G), \pi)$. Let

$$\pi((m, e_1, \cdots, e_N, f_1, \cdots, f_n)) = (pm, pe_1, \cdots, pe_N).$$

Then the following maps Φ make $(B, B(X), \Delta(G), \Delta(G), \pi)$ into a bundle: If ϕ is a strip map of the bundle (M, X, F, G, p), then

$$\Phi((x, \bar{e}_1, \cdots, \bar{e}_N), (f, A_1(f), \cdots, A_n(f)) = (\phi(x, f), e_1, \cdots, e_N, \phi_x A_1(f), \cdots, \phi_x A_n(f)).$$

Here, the e_i are 'horizontal' (with respect to the M-metric) vectors at $\phi(x, f)$ which project into the $\bar{e}_i$ under p.

Proof that these Φ are strip maps. If ϕ is defined on a submanifold U of X and U' denotes the set of all points x of $B(X)$ with $p_X(x) \in U$, then Φ maps $U' \times \Delta(G)$ 1-1 onto $\pi^{-1}(U')$, with Φ and its inverse both C^∞. Also, any two such maps Φ, Φ' differ along a fibre $\pi^{-1}((x, \bar{e}_1, \cdots, \bar{e}_N))$ by a translation $L_{\Delta(g)}$; and, in fact, g depends on x, but is independent of the frame $\bar{e}_1, \cdots, \bar{e}_N$ at x.

$(B, X, O(X) \times \Delta(G), O(X) \times \Delta(G), p_X \circ \pi)$. The following maps $\bar{\Phi}$ make this into a bundle: If ϕ^X is a strip map of $\mathfrak{B}(X)$ and Φ is a strip map of $(B, B(X), \Delta(G), \Delta(G), \pi)$, then $\bar{\Phi}(x, r \times \Delta(g)) = \Phi(\phi^X(x, r), \Delta(g))$, $r \in O(X)$. The $\bar{\Phi}$'s are strip maps, since any two differ along a fibre by a translation of $O(X) \times \Delta(G)$ (this is a consequence of the fact that the element $\Delta(g)$ of the preceding paragraph is independent of the frame at x, i.e., independent of r).

LEMMA 1. *Let $\phi, \phi^X, \phi^X, \phi^M$ be strip maps of the bundles (M, X, F, G, p), $\mathfrak{B}(X), \mathfrak{B}(F), \mathfrak{B}(M)$; let Φ be the strip map of $(B, B(X), \Delta(G), \Delta(G), \pi)$ defined as above in terms of ϕ. Then:*

(1) *given ϕ, ϕ^X on θ^X, and ϕ^F on θ^F, (θ^X, θ^F submanifolds of X, F) there exists a ϕ^M on $\phi(\theta^X, \theta^F)$ such that $\phi^M(\phi(x, f), r \oplus \Delta) = \Phi(\phi^X(x, r), \phi^F(f, \Delta))$ for any $x \in \theta^X$, $f \in \theta^F$, and $r \oplus \Delta \in O(X) \oplus \Delta(K)$;*

(2) *give ϕ^M on some submanifold θ^M of M, there exist ϕ, ϕ^X on some θ^X, and ϕ^F on some θ^F, such that $\phi(\theta^X, \theta^F) \subset \theta^M$ and $\phi^M(\phi(x, f), r \oplus \Delta) = \Phi(\phi^X(x, r), \phi^F(f, \Delta))$ for any $x \in \theta^X$, $f \in \theta^F$, and $r \oplus \Delta \in O(X) \oplus \Delta(K)$.*

Proof. This is a consequence of the definition of Φ in terms of ϕ, and of the type of strip map ϕ^M considered in $\mathfrak{B}(M)$.

Curvature. A choice of coordinates x_i', y_i' in neighborhoods in X, F, and a strip map ϕ of the bundle (M, X, F, G, p), define coordinates on an M-neighborhood. These, together with coordinates s_i', t_i' on $O(X)$ and $\Delta(K)$ and a strip map ϕ^M of $\mathfrak{B}(M)$, define coordinates x_i, y_i, s_i, t_i on a submanifold of B. We denote partial derivatives in the coordinate directions by X_i, Y_i, S_i, T_i. Then a change of coordinates or strip maps (new coordinates being denoted by bars) sends each S_i into a linear combination of the $\bar{S}_j$, each T_i into a linear combination of the $\bar{T}_j$, and each Y_i into a linear combination of the $\bar{Y}_j$ and $\bar{T}_j$ (the Y_j and T_j span the space of vertical vectors of B with respect to the bundle $(B, B(X), \Delta(G), \Delta(G), \pi)$, as do the $\bar{Y}_j$ and $\bar{T}_j$.)

If $\tilde{m}$ is a point of B and $m = p_M(\tilde{m})$, then $S_i(\tilde{m}) = \phi_m{}^M(t \oplus 0)$ for some strip map ϕ^M of $\mathfrak{B}(M)$ and some vector t of $O(X)$. Conversely, every vector of the form $\phi_m{}^M(t \oplus 0)$ is a linear combination of the S_j.

Notation. A point $(m, e_1, \cdots, e_N, f_1, \cdots, f_n)$ will be denoted by (m, e_i, f_i); similarly, points $(x, e_1, \cdots, e_N)$ and $(f, f_1, \cdots, f_n)$ will be denoted by (x, e_i) and (f, f_i).

LEMMA 2. *Let Δg be an element of $\Delta(G)$ and $\tilde{m}$ a point of B. Then $R_{\Delta g} S_i(\tilde{m}) = S_i(R_{\Delta g}\tilde{m})$.*

Proof. Let $m = p_M(\tilde{m})$, $m' = p_M(R_{\Delta g}\tilde{m})$. So, for some strip map ϕ of (M, X, F, G, p) and some $\bar{g}K \in F$, $\tilde{m} = (\phi(x, \bar{g}K), e_i(m), \phi_x A_i(\bar{g}K))$. Letting $\bar{e}_i = pe_i(m)$, it follows that $\tilde{m} = \Phi((x, \bar{e}_i), (\bar{g}K, A_i(\bar{g}K)))$, and hence that

$$R_{\Delta g}(\tilde{m}) = \Phi((x, \bar{e}_i), (\bar{g}gK, A_i(\bar{g}gK))) = (\phi(x, \bar{g}gK), e_i(m'), \phi_x A_i(\bar{g}gK)).$$

Thus we have

$$(*): R_{\Delta g}(\phi(x, \bar{g}K), e_i(m), \phi_x A_i(\bar{g}K)) = (\phi(x, \bar{g}gK), e_i(m'), \phi_x(\bar{g}gK)),$$

with $pe_i(m) = pe_i(m') = \bar{e}_i$. (Note that $m = \phi(x, \bar{g}K)$ and $m' = \phi(x, \bar{g}gK)$.) It follows immediately from the definition of the coordinates s_i in terms of the strip maps of $\mathfrak{B}(M)$ that $pe_i(m) = pe_i(m')$ implies $s_i \circ R_{\Delta g} = s_i$ for all i (for, if $\bar{e}_i = \Sigma c_{ij}\mathfrak{a}_j$, then $e_i(m) = \Sigma c_{ij}\mathfrak{a}_j'(m)$ and $e_i(m') = \Sigma c_{ij}\mathfrak{a}_j'(m')$). Thus equation $(*)$ shows that $R_{\Delta g} S_i = S_i$, since the x_j, y_j, t_j coordinates of $R_{\Delta g}(\tilde{m})$ can be seen to depend only on the x_j, y_j, t_j coordinates of $\tilde{m}$, not on the s_j coordinates of $\tilde{m}$.

LEMMA 3. *There exists a connection ω on $(B, B(X), \Delta(G), \Delta(G), \pi)$ satisfying:*

(a) $\omega(S_i(m)) = 0$ *for all i and all $m \in B$;*

(b) $R_{r \oplus \epsilon}\omega = \omega$ ($r \oplus \epsilon$ *in* $O(X) \oplus \Delta(K)$, $\epsilon = \Delta$ (*identity element of* G)).

Proof. A preliminary concept of horizontality H_o on B with respect to the bundle $(B, B(X), \Delta(G), \Delta(G), \pi)$ can be defined by $H_o S_i = S_i$, $H_o T_i = 0$, $H_o Y_i = 0$; this is independent of the coordinates. Let $V_o = I - H_o$, I the identity. Note that $H_o X_i$ is undefined.

Let H be a connection (concept of horizonality) on B with respect to the bundle $(B, X, O(X) \times \Delta(G), O(X) \times \Delta(G), p_X \circ \pi)$; let $\hat{V} = I - \hat{H}$. For any tangent vector Z at a point of B, define HZ and VZ as follows:

1. $VZ = V_o(VZ)$

2. $HZ = Z - VZ.$

So HZ and VZ are well-defined, and $VZ = V_oZ$ if Z is an S_i, T_i, or Y_i.

To prove that H is a connection on $(B, B(X), \Delta(G), \Delta(G), \pi)$, it must be shown that $R_{\Delta g}Z$ is H-horizontal for any $\Delta g \in \Delta(G)$ and any H-horizontal vector Z on B. So suppose Z is H-horizontal. Then Z is either $\hat{H}$-horizontal, or it is a linear combination of S_i's, or both. If Z is H-horizontal, then $V(R_{\Delta g}Z) = V_o(VR_{\Delta g}Z) = 0$ since $R_{\Delta g}$ preserves $\hat{H}$-horizontality; and if Z is a linear combination of S_i's, Lemma 2 shows that $V(R_{\Delta g}Z) = V_o(\hat{V}(R_{\Delta g}Z)) = V_o(R_{\Delta g}Z) = 0$.

Thus H is a connection; let ω be the 1-form of H. Then $\omega(S_i) = 0$, and it must still be shown that $R_{r\oplus\epsilon}{}^*\omega = \omega$. So suppose Z is a tangent vector at a point $\bar{m} = (m, e_i, f_i)$ of B. Let $x = pm$, and let ϕ be a strip map of (M, X, F, G, p) with $m = \phi(x, f)$; choose vectors $\bar{f}_i$ at f with $\phi_x\bar{f}_i = f_i$. Let Φ be the strip map of $(B, B(X), \Delta(G), \Delta(G)\pi)$ associated with ϕ, and define p_ϕ by: $p_\phi(\phi(x', f'), e_i', \phi_x f_i') = (f', f_i')$, for any point $(\phi(x', f'), e_i', \phi_x f_i')$. Then $\omega(Z)$ is the invariant vector field on $\Delta(G)$ whose value at the point $p_\phi(\bar{m})$ is $p_\phi V(Z)$. Now every $R_{r\oplus\epsilon}$ maps H-horizontal vectors into H-horizontal vectors, and V-vertical vectors into V-vertical vectors (since $\pi \circ R_{r\oplus\epsilon} = R_r \circ \pi$). Thus $R_{r\oplus\epsilon} \circ V = V \circ R_{r\oplus\epsilon}$. Furthermore, $p_\phi \circ R_{r\oplus\epsilon} = p_\phi$. Thus $\omega(R_{r\oplus\epsilon}Z) = p_\phi V R_{r\oplus\epsilon}Z = p_\phi R_{r\oplus\epsilon} VZ = p_\phi VZ = \omega(Z)$.

Let ω_X be a connection on $\mathfrak{B}(X)$ with curvature form Ω_X, and let ω be a connection on $(B, B(X), \Delta(G), \Delta(G), \pi)$ which satisfies the two properties of Lemma 3; let Ω be the curvature form of ω. Define $\omega^*(\mathrm{ad}\,\Omega_F)$, $\omega^*(\mathrm{ad}\,\Omega_F)$ and $\Omega^*(\mathrm{ad}\,\omega_f)$ in the following way: $\omega^*\,\mathrm{ad}\,\omega_F(Z) = \mathrm{ad}\,\omega_F(\omega Z)$, $\omega^*\,\mathrm{ad}\,\Omega_F(Z, Z') = \mathrm{ad}\,\Omega_F(\omega Z, \omega Z')$, and $\Omega^*\,\mathrm{ad}\,\omega_F(Z, Z') = \mathrm{ad}\,\omega_F(\Omega(Z, Z'))$. These are well-defined, since the canonical connection of the second kind $\mathrm{ad}\,\omega_F$, and its curvature form $\mathrm{ad}\,\Omega_F$, are invariant under left-translations by $\Delta(G)$.

THEOREM 1. *$\bar{\omega} = \pi^*\omega_X \oplus \omega^*\,\mathrm{ad}\,\omega_F$ is a connection on $\mathfrak{B}(M)$. Its curvature form is $\bar{\Omega} = \pi^*\Omega_X \oplus (\omega^*\,\mathrm{ad}\,\Omega_F + \Omega^*\,\mathrm{ad}\,\omega_F)$.*

Proof. First, it must be shown that $\bar{\omega}$ behaves correctly under right-translations by $O(X) \oplus \Delta(K)$. So let I be the unit matrix of $O(X)$, and $r \oplus \Delta$ any element of $O(X) \oplus \Delta(K)$. Since $\pi \circ R_{r\oplus\Delta} = R_r \circ \pi$ and $\omega \circ R_{r\oplus\epsilon} = \omega$, and since ω_X and $\mathrm{ad}\,\omega_F$ are themselves connections, we have

$$\begin{aligned} R_{r\oplus\Delta}{}^*\bar{\omega} &= \omega_X(\pi R_{r\oplus\Delta}) \oplus \mathrm{ad}\,\omega_F(\omega R_{r\oplus\Delta}) = \omega_X(R_r\pi) \oplus \mathrm{ad}\,\omega_F(\omega R_{I\oplus\Delta}) \\ &= \omega_X(R_r\pi) \oplus \mathrm{ad}\,\omega_F(\mathrm{ad}\,\Delta^{-1}\omega) = \omega_X(R_r\pi) \oplus \mathrm{ad}\,\omega_F(R_\Delta\omega) \\ &= \mathrm{ad}\,r^{-1}(\omega_X \circ \pi) \oplus \mathrm{ad}\,\Delta^{-1}(\mathrm{ad}\,\omega_F \circ \omega) = \mathrm{ad}(r \oplus \Delta)^{-1}\bar{\omega}. \end{aligned}$$

Next, let $\phi^M(m, r \oplus \Delta) = \tilde{m}$ be a point of B, and let $\tilde{A} \oplus \tilde{B}$ be an element of the Lie algebra of $O(X) \oplus \Delta(K)$ with value $\alpha \oplus \beta$ at the point $r \oplus \Delta$. It must be shown that $\bar{\omega}(\phi_m{}^M(\tilde{\alpha} \oplus \beta)) = \tilde{A} \oplus \tilde{B}$. So let ϕ, ϕ^X, ϕ^F be the strip maps whose existence is guaranteed by Lemma 1, and let $\tilde{x}$, x, f be the points of $B(X)$, X, F satisfying $\pi(\tilde{m}) = \tilde{x}$ and $\phi(x,f) = p_M(\tilde{m})$; let $m = p_M(\tilde{m})$. Since $\phi_m{}^M(\alpha \oplus 0)$ is a linear combination of (H-horizontal) S_i's, it follows that $V\phi_m{}^M(\alpha \oplus \beta) = \phi_m{}^M(0 \oplus \beta)$. Thus:

$$\begin{aligned}\bar{\omega}(\phi_m{}^M(\alpha \oplus \beta)) &= \omega_X(\pi\phi_m{}^M(\alpha \oplus \beta)) \oplus \operatorname{ad}\omega_F(\omega\phi_m{}^M(\alpha \oplus \beta))\\ &= \omega_X(\pi\phi(\phi_x{}^X(\alpha), \phi_f{}^F(\beta)) \oplus \operatorname{ad}\omega_F(\omega\phi_m{}^M(0 \oplus \beta))\\ &= \omega_X(\phi_x{}^X(\alpha)) \oplus \operatorname{ad}\omega_F(\omega\phi(0, \phi_f{}^F(\beta)) = \omega_X(\phi_x{}^X(\alpha)) \oplus \operatorname{ad}\omega_F(\lambda),\end{aligned}$$

where λ is the left-invariant vector field on $\Delta(G)$ whose value at f is $\phi_f{}^F(\beta)$. Since ω_X and $\operatorname{ad}\omega_F$ are connections, it follows that $\bar{\omega}(\phi_m{}^M(\alpha \oplus \beta)) = \tilde{A} \oplus \tilde{B}$.

Thus, $\bar{\omega}$ is a connection on $\mathfrak{B}(M)$.

The equation of structure gives the following expression for $\bar{\Omega}$:

$$\begin{aligned}\bar{\Omega} &= d\bar{\omega} + (\tfrac{1}{2})\bar{\omega} \wedge \bar{\omega}\\ &= (d\pi^*\omega_X \oplus d\omega^* \operatorname{ad}\omega_F) + (\tfrac{1}{2})(\pi^*\omega_X \wedge \pi^*\omega_X \oplus \operatorname{ad}\omega_F \wedge \omega^* \operatorname{ad}\omega_F)\\ &= (\pi^* d\omega_X + (\tfrac{1}{2})\pi^*\omega_X \wedge \pi^*\omega_X) \oplus (d\omega^* \operatorname{ad}\omega_F + (\tfrac{1}{2})\omega^* \operatorname{ad}\omega_F \wedge \omega^* \operatorname{ad}\omega_F)\\ &= (\pi^*\Omega_X) \oplus (\omega^* \operatorname{ad}\Omega_F + (d \circ \omega^* - \omega^* \circ d)\operatorname{ad}\omega_F).\end{aligned}$$

Let Ω be the curvature form of ω; then $\Omega^* = d \circ \omega^* - \omega^* \circ d$ (see [2]), and so Theorem 1 is proved.

Thus $\bar{\omega}$ is a connection on the frame bundle of M. If K is connected, $\Delta(K)$ is contained in the rotation group $R(n)$; and so if ω_X is chosen to be a connection on the bundle of oriented frames of X, then $\bar{\omega}$ is a connection on the bundle of oriented frames of M.

If G/K is any reductive homogeneous space (that is, G is a Lie group and there exists a complement $\mathfrak{m}$ to the Lie algebra of K in the Lie algebra of G), then one can proceed as follows: Let B_X, B_F be the bundles of bases of X, F; and let B_M' be the set of all elements $(m, e_1, \cdots, e_N, f_1, \cdots, f_n)$, with $m \in M$, $e_1, \cdots, e_N$ a set of linearly independent tangent vectors at m which are horizontal (with respect to (M, X, F, G, p)), and $f_1, \cdots, f_n$ a set of linearly independent vertical tangent vectors at m. Then, on the bundle (B_M', B_X, B_F, G, π)—G acts in the natural way—ω is defined as before; however, this bundle is not a principal bundle, and so, strictly speaking, ω is not a connection. If ω_X is a connection on the bundle of bases of X, and if Ω^* denotes $d \circ \omega^* - \omega^* \circ d$, then $\bar{\omega} = \pi^*\omega_X \oplus \omega^* \operatorname{ad}\omega_F$ is a connection on the bundle of bases of M, with curvature form $\bar{\Omega} = \pi^*\Omega_X \oplus (\omega^* \operatorname{ad}\Omega_F + \Omega^* \operatorname{ad}\omega_F)$. In this case, of course, $\operatorname{ad}\omega_F$ is a connection on B_F.

The characteristic ring of *M*. From now on, K will be assumed to be connected.

Define tensors $T_r{}^X$, $T_r{}^F$, and $T_r{}^M$, on $O(X)$, $O(F)$, and $O(M)$ as follows:

(a) $T_r{}^X(A,\cdots,C)=\Sigma\epsilon a_{i_1j_1}\cdots c_{i_rj_r}$ ($A=(a_{ij}),\cdots,C=(c_{ij})$ *are* r $N\times N$ skew-symmetric matrices; $i_1,\cdots,i_r$ is any set of r numbers from among $1,\cdots,N$; $j_1,\cdots,j_r$ is any permutation of $i_1,\cdots,i_r$; ϵ is the sign of the permutation; and the summation extends over all such permutations, and all choices of $i_1,\cdots,i_r$.)

(b) $T_r{}^F(A,\cdots,C)=\Sigma\epsilon a_{i_1j_1}\cdots c_{i_rj_r}$ ($A,\cdots,C$ are r $n\times n$ skew-symmetric matrices; $i_1,\cdots,i_r$ is any set of r numbers from among $1,\cdots,n$)

(c) $T_r{}^M(A,\cdots,C)=\Sigma\epsilon a_{i_1j_1}\cdots c_{i_rj_r}$ ($A,\cdots,C$ are r $v\times v$ skew-symmetric matrices, v the dimension of M; $i_1,\cdots,i_r$ is any set r numbers from among $1,\cdots,v$.)

Then $\bar T_r{}^X(\Omega_X,\cdots,\Omega_X)$, $\bar T_r{}^F(\Omega_F,\cdots,\Omega_F)$, and $\bar T_r{}^M(\bar\Omega,\cdots,\bar\Omega)$ are $2r$-forms on $B(X)$, $\Delta(G)$, and B (the bars denote alternation with respect to the vector arguments). They define differential forms $P_r{}^X$, $P_r{}^F$, and $P_r{}^M$ on X, F, and M, with $p_X{}^*P_r{}^X=\bar T_r{}^X(\Omega_X,\cdots,\Omega_X)$, $p_FP_r{}^F=\bar T_r{}^F(\Omega_F,\cdots,\Omega_F)$, and $p_M{}^*P_r{}^M=\bar T_r{}^M(\bar\Omega,\cdots,\bar\Omega)$. A fundamental theorem of Weil shows that these differential forms are independent of the choice of connections on $\mathfrak{B}(X)$, $\mathfrak{B}(F)$, and $\mathfrak{B}(M)$.

Definition. $P_r{}^X$, $P_r{}^F$, $P_r{}^M$ are the *2r-th Pontrjagin characteristic forms* of X, F, and M.

LEMMA 4.

$$\begin{aligned}&\bar T_r{}^M(\bar\Omega,\cdots,\bar\Omega)\\&\quad=\Sigma_j\bar T_j{}^X(\pi^*\Omega_X,\cdots,\pi^*\Omega_X)\\&\qquad\wedge\bar T_{r-j}{}^F(\omega^*\operatorname{ad}\Omega_F+\Omega^*\operatorname{ad}\omega_F,\cdots,\omega^*\operatorname{ad}\Omega_F+\Omega^*\operatorname{ad}\omega_F).\end{aligned}$$

Proof. This is a direct consequence of Theorem 1.

Interpretation of

$$\boldsymbol{\bar T_r{}^F(\omega^*\operatorname{ad}\Omega_F+\Omega^*\operatorname{ad}\omega_F,\cdots,\omega^*\operatorname{ad}\Omega_F+\Omega^*\operatorname{ad}\omega_F)}.$$

M' gives rise to a space B' in a manner analogous to the manner in which M gave rise to the space B. We can consider G as a homogeneous space G/e; then G is a bundle over G/e, with fibre e, and we consider the

following horizontal orthonormal left-invariant vector fields on G (note that all vector fields on G are horizontal, since the fibre is e): $X_1, \cdots, X_n$ are to be horizontal at every point with respect to the connection ω_F of $(G, G/K, K, K, \delta)$; $X_{n+1}, \cdots, X_m$— m the dimension of G—are to be vertical at every point, with respect to ω_F. Clearly, $\Delta(G) = G \times e$ for the bundle $(G, G/e, e, e, I)$; hence $(B', B(X), G, G, \pi')$, π' the natural projection of B' onto $B(X)$, is the bundle which corresponds to the bundle

$$(B, B(X), \Delta(G), \Delta(G), \pi).$$

Let p_M' be the natural projection of B' onto M'. If we choose $X_1, \cdots, X_n$ to be the same vector fields on G as the ones which defined $\Delta(G)$ in the case of the bundle $(B, G/K, K, K, \delta)$, we get a natural mapping P_o of B' into B: Let ϕ be a strip map of (M, X, F, G, p), ϕ' andΦ the associated strip maps of (M', X, G, G, p') and $(B, B(X), \Delta(G), \Delta(G), \pi)$, and Φ' the strip map of $(B', B(X), G, G, \pi')$ associated with ϕ'. Then let $P_o(\Phi'(b(x), g)) = \Phi(b(x), \Delta g)$, $b(x) \in B(X)$ and $g \in G$.

Note. Another way of defining this mapping is the following: If $\bar{m}' = (m', e_1', \cdots, e_N', f_1', \cdots, f_n', f_{n+1}', \cdots, f_m')$ is a point of B', then $P_o(\bar{m}')$ is the point $(Pm', Pe_1', \cdots, Pe_N', Pf_1', \cdots, Pf_n')$.

The following diagram is commutative $(P \circ p_M' = p_M \circ P_o)$:

$$\begin{array}{ccc} B & \xleftarrow{\quad P_o \quad} & B' \\ {\scriptstyle p_M}\big\downarrow & & \big\downarrow{\scriptstyle p_M'} \\ M & \xleftarrow{\quad P \quad} & M' \end{array}$$

One can construct a connection ω' on $(B', B(X), G, G, \pi')$ in a manner analogous to the construction of ω in Lemma 3. Then it can easily be seen that there is a connection ω on $(B, B(X), \Delta(G), \Delta(G), \pi)$ which satisfies the conditions of Lemma 3 and which satisfies the further condition: $P_o{}^*\omega = \Delta \circ \omega'$. It follows from the equation of structure that $P_o{}^*\Omega = \Delta \circ \Omega'$.

Hereafter, the connections ω and ω' will remain fixed, chosen as in the preceding paragraph.

Let $s_1 = \omega^* \operatorname{ad} \Omega_F + \Omega^* \operatorname{ad} \omega_F$. Then s_i is $\bar{H}$-horizontal on B, and $R_{r \oplus \Delta}{}^* s_1 = \operatorname{ad}(r \oplus \Delta)^{-1} s_1$, $r \oplus \Delta \in O(X) \oplus \Delta(K)$.

Let S_1 be the following linear-transformation valued 2-form on M: If t, t' are tangent vectors at a point m of M, and if T, T' are tangent vectors at a point $(m, e_1, \cdots, e_N, f_1, \cdots, f_n)$ of B with $p_M T = t$ and $p_M T' = t'$,

then $S_1(t,t')$ is the linear transformation of the tangent space to M at m whose matrix with respect to the basis $e_1,\cdots,e_N,f_1,\cdots,f_n$ is $s_1(T,T')$.

Thus $\bar{T}_r^F(s_1,\cdots,s_1)=p_M{}^*\bar{T}_r^F(S_1,\cdots,S_1)$.

LEMMA 5. *Let* $s_2=\omega'^*\Omega_F+\Omega'^*\omega_F$. *Then* $P_o{}^*s_1=\Delta\circ s_2$.

Proof. $P_o{}^*s_1=P_o{}^*(\omega^*\operatorname{ad}\Omega_F+\Omega^*\operatorname{ad}\omega_F)=\operatorname{ad}\Omega_F(\omega\circ P_o)+\operatorname{ad}\omega_F(\Omega\circ P_o)$ $=\operatorname{ad}\Omega_F(\Delta\circ\omega')+\operatorname{ad}\omega_F(\Delta\circ\Omega')=\Delta(\Omega_F\omega'+\omega_F\Omega')=\Delta\circ s_2$. (The second-to-last equality follows from the definition of the connection $\operatorname{ad}\omega_F$ in terms of ω_F and Δ.)

Definition. T_r^F defines a tensor t_r^F on K in the following way: If $X,\cdots,Z$ are r elements of the Lie algebra of K, then $t_r^F(X,\cdots,Z)$ $T_r^F(\operatorname{ad}X[\mathfrak{m}],\cdots,\operatorname{ad}Z[\mathfrak{m}])$ (recall that the Lie algebra of G splits, with respect to the fundamental bilinear form, into the direct sum of the Lie algebra of K and its orthogonal complement $\mathfrak{m}$.) Since K is connected, t_r^F is invariant under K.

Now each tensor t_r^F gives rise to a characteristic form p_r^F of M with respect to the bundle (M',M,K,K,p). We have:

LEMMA 6. *The forms* $\bar{T}_r^F(S_1,\cdots,S_1)$ *and* p_r^F *are cohomologous on* M.

Proof. It will be shown that there is a curvature form $\bar{\Omega}$ on the bundle (M',M,K,K,P) for which $p^*\bar{T}_r^F(S_1,\cdots,S_1)=\bar{t}_r^F(\bar{\Omega},\cdots,\bar{\Omega})$; this will prove the lemma. It is equivalent, however, to show that $p_M{}'^*\bar{t}_r^F(\bar{\Omega},\cdots,\bar{\Omega})$ $=P_o{}^*\bar{T}_r^F(s_1,\cdots,s_1)$. Now it follows from Lemma 5 that $P_o{}^*\bar{T}_r^F(s_1,\cdots,s_1)$ $=\bar{t}_r^F(s_2,\cdots,s_2)$, since $\Delta(Z)=\operatorname{ad}Z[\mathfrak{m}]$ for any Z in the Lie algebra of K; hence it must be shown that $p_M{}'^*\bar{t}_r^F(\bar{\Omega},\cdots,\bar{\Omega})=\bar{t}_r^F(s_2,\cdots,s_2)$. We will now prove, in fact, that $\bar{\Omega}$ can be so chosen that $p_M{}'^*\bar{\Omega}=s_2$.

We define a connection H'' on (M',X,G,G,p') by the condition $p_M{}'\circ H'$ $=H''\circ p_M{}'$. This is well-defined; and if ω'' is the 1-form of H'', it will be shown in the following paragraph that $\omega'=p_M{}'^*\omega''$. Thus the equation of structure shows that $\Omega'=p_M{}'^*\Omega''$. Now $\omega_F\circ\omega''$ is a connection on the bundle (M',M,K,K,P); let $\bar{\Omega}$ be its curvature form. Then it follows from the equation of structure that $\bar{\Omega}=\omega''^*\Omega_F+\Omega''^*\omega_F$. Thus

$$p_M{}'^*\bar{\Omega}=\omega'^*\Omega_F+\Omega'^*\omega_F=s_2.$$

Proof that $\omega'=p_M{}'^*\omega''$. Let ϕ be a strip map of (M,X,F,G,p), let ϕ' be the associated strip map of (M,X,G,G,p'), and let Φ be the associated strip map of $(B,B(X),\Delta(G),\Delta(G),\pi)$; let Φ' be the strip map of $(B',B(X),G,G,\pi')$ associated with ϕ'.

(a) $p_M' \circ V' = V'' \circ p_M'$ (where $H' + V' = I$ and $H'' + V'' = I$). For any vector Y of B',

$$p_M'H'Y + p_M'V'Y = p_M'Y = H''p_M'Y + V''p_M'Y = p_M'H'Y + V''p_M'Y,$$

hence $p_M'V'(Y) = V''p_M'(Y)$.

(b) Let $b(x)$ be a point of $B(X)$ and g a point of G; then

$$p_M'\Phi'(b(x), g) = p_M'(\phi'(x,g), e_i, \phi_x'A_i(g)) = \phi'(x,g),$$

(c) $\phi_x'^{-1} \circ p_M' = \Phi_{b(x)}'^{-1}$ on $\pi'^{-1}(b(x))$. Let $\bar{m}' = \Phi'(b(x),g)$ be a point of B'. So $\Phi_{b(x)}'^{-1}(\bar{m}') = g$, and it follows from (b) that $\phi_x'^{-1}p_M'(\bar{m}') = \phi_x'^{-1}(\phi'(x,g)) = g$.

We now show that $\omega' = \omega'' \circ p_M'$ on H'-horizontal and H'-vertical vectors of B', thus completing the proof. If Z is H'-horizontal, then $\omega'(Z) = \omega''(p_M'Z) = 0$. If Z is H'-vertical, it follows from (a) that $p_M'Z$ is H''-vertical; thus, if Z lies in the fibre above the point $b(x)$ of $B(X)$, it follows from (c) that $\omega''(p_M'Z) = \phi_x'^{-1}p_M'(V'Z) = \Phi_{b(x)}'^{-1}(V'Z) = \omega'(V'Z)$ (where, of course, the two middle terms are extended to left-invariant vector fields).

THEOREM 2. *For any positive integer r, $P_r^M = \Sigma_j p^*P_j^X \wedge p_{r-j}^F$, where P_r^M, P_j^X are the Pontrjagin forms of M, X, and where p_{r-j}^F is the characteristic form on M defined by the tensor t_{r-j}^F on K.*

Proof. $\bar{T}_j^X(\Omega_X, \cdots, \Omega_X) = p_X^*P_j^X$, where p_X is the projection of $B(X)$ onto X; thus $\pi^*(\bar{T}_j^X(\Omega_X, \cdots, \Omega_X)) = \pi^*p_X^*P_j^X$. Now $p_X \circ \pi = p \circ p_M$; and so it follows from Theorem 1 and Lemma 6 that:

$$p_M^*P_r^M = \bar{T}_r^M(\bar{\Omega}, \cdots, \bar{\Omega}) = \Sigma_j p_M^*p^*P_j^X \wedge p_M^*p_{r-j}^F = p_M^*(\Sigma_j p^*P_j^X \wedge p_{r-j}^F).$$

Thus $P_r^M = \Sigma_j p^*P_j^X \wedge p_{r-j}^F$.

Remark. The bundle (M', M, K, K, p) and the mapping Δ of K into $O(n)$ induce a principal bundle over M with fibre and group $O(n)$. So p_r^F is the $2r$-th Pontrjagin form of M with respect to this bundle. It is known that the Pontrjagin forms of degree greater than $2n$ of a principal bundle with group $O(n)$ are zero; bundle; hence $p_s^F = 0$ if $s > 2n$.

COROLLARY. *If the characteristic ring of M with respect to the bundle (M', M, K, K, P) is empty, then:*

(a) $P_r^M = p^*P_r^X$ *if $r \leq$ dimension of X;*

(b) $P_r^M = 0$ *if $r >$ dimension of X.*

This holds in particular when K is a normal subgroup of G.

Proof. Only the second part of this corollary remains to be proved. If K is a normal subgroup of G, let f be a cross-section of G/K into G, and let f' be the following mapping of M into M': $f'(\phi(x, gK)) = \phi'(x, f(gK))$. So f' is defined in terms of strip maps, but is clearly independent of the strip map used; it is a cross-section of M into M', and hence the characteristic ring of M with respect to the bundle (M', M, K, K, P) is empty.

PRINCETON UNIVERSITY.

REFERENCES.

[1] W. Ambrose and I. M. Singer, "A theorem on holonomy," *Transactions of the American Mathematical Society*, vol. 75 (1943), pp. 428-443.

[2] H. Cartan, *Colloque de Topologie* (*espaces fibrés*), Bruxelles, 1950, Liège et Paris, 1951, pp. 15-27 and 57-71.

[3] S. S. Chern, *Topics in Differential Geometry*, Institute for Advanced Study, Princeton, 1951 (mimeographed notes).

ON MAPS FROM SPHERES TO EUCLIDEAN SPACES.*

By Chung-Tao Yang.

1. Introduction. Knaster [1] proposed the following problem: Given a map (= continuous function) f of an $(m+n-2)$-sphere S^{m+n-2} into the euclidean n-space and m distinct points $x_1, \cdots, x_m$ of S^{m+n-2}, does there exist a rotation r of S^{m+n-2} such that $f(r(x_1)) = \cdots = f(r(x_m))$? Up to the present we know only several partial solutions of this problem. For the case $n = 2$, a positive answer follows from the generalized Borsuk-Ulam's theorem by Hopf [2]. If $m = 3$, $n = 1$ and x_1, x_2, x_3 are end points of three mutually orthogonal radii, a positive answer can be found in Kakutani [3]. The result of Kakutani was extended by both Yamabe-Yujobô [4] and Floyd [5]. The former removed the restriction on m and the latter removed the restriction on x_1, x_2, x_3. The purpose of this note is to extend the result of Kakutani by removing the restriction on n and weakening the restriction on x_1, x_2, x_3. In fact, we shall prove

Theorem 1. *Given a number d, $0 < d \leqq 2\pi/3$, and a map f of an $(n+1)$-sphere S^{n+1} into the euclidean n-space, there exist three points x_1, x_2, x_3 of S^{n+1} such that $f(x_1) = f(x_2) = f(x_3)$ and the spherical distance between any two of x_1, x_2, x_3 is equal to d.*

Notice that Theorem 1 and Floyd [5] give a strong indication that for the case $m = 3$ the answer to Knaster's problem is probably in the affirmative. The proof of Theorem 1 is roughly as follows. Let X_d be the subset of $S^{n+1} \times S^{n+1} \times S^{n+1}$ consisting of all the elements (x_1, x_2, x_3) such that the spherical distance between any two of x_1, x_2, x_3 is equal to d. If there is a map f of S^{n+1} into the euclidean n-space such that for no $(x_1, x_2, x_3) \in X_d$, $f(x_1) = f(x_2) = f(x_3)$, we shall construct a map g of X_d into a $(2n-1)$-sphere S^{2n-1} and a subset Y of X_d which is topologically a cylinder with the Stiefel manifold $V_{n+1,2}$ as its base. Then we arrive at a contradiction by proving that g is essential when restricted on one base of Y but is inessential when restricted on the other. For the case $n = 1$, Y consists of two circular

* Received May 8, 1957.

cylinders. If Y is replaced by either of these two cylinders, the proof we have is essentially the same as that in [3].

As in [2], the same proof yields a generalized theorem concerning maps from Riemannian manifolds to euclidean spaces.

2. Preliminaries. Throughout this note, n denotes a positive integer and R^n denotes the euclidean n-space. Let S^{n+1} be an $(n+1)$-sphere with center o. Whenever $x, y \in S^{n+1}$, $\rho(x,y)$ denotes the spherical distance between x and y, i.e., the angle between the vectors ox and oy. Clearly ρ is a Riemannian metric on S^{n+1} and geodesics are arcs of great circles of S^{n+1}. If x_1, x_2, x_3 are three distinct points of S^{n+1} such that $\rho(x_2,x_3)=\rho(x_3,x_1)=\rho(x_1,x_2)=d$, then $0<d\leqq 2\pi/3$.

For any fixed number d, $0<d\leqq 2\pi/3$, we let X_d be the subset of $S^{n+1}\times S^{n+1}\times S^{n+1}$ consisting of all the elements (x_1,x_2,x_3) such that $\rho(x_2,x_3)=\rho(x_3,x_1)=\rho(x_1,x_2)=d$. The elements of X_d are called *d-triples* on S^{n+1}.

If $d<2\pi/3$, there is a natural homeomorphism between X_d and the Stiefel manifold $V_{n+2,3}$ consisting of all the orthogonal 3-frames with o as the origin. In fact, any $(x_1,x_2,x_3)\in X_d$ determines an orthogonal 3-frame (oy, oy_2, oy_3) as follows. oy_1 is the unit vector on ox_1. oy_2 is the unit vector on the 2-plane $[ox_1x_2]$ orthogonal to oy_1 and such that the projection of ox_2 on oy_2 is positive. oy_3 is the unit vector on the 3-plane $[ox_1x_2x_3]$ orthogonal to the 2-plane $[ox_1x_2]$ and such that the projection of ox_3 on oy_3 is positive. The correspondence $(x_1,x_2,x_3)\to(oy_1,oy_2,oy_3)$ is clearly a desired homeomorphism. If $d=2\pi/3$, then for every $(x_1,x_2,x_3)\in X_d$, x_1, x_2, x_3 are on a great circle of S^{n+1}. Therefore x_3 is on the 2-plane $[ox_1x_2]$ and is determined by x_1, x_2. Just as above, the d-triple (x_1,x_2,x_3) determines an orthogonal 2-frame (oy_1,oy_2) and the correspondence $(x_1,x_2,x_3)\to(oy_1,oy_2)$ gives a homeomorphism of $X_{2\pi/3}$ onto the Stiefel manifold $V_{n+2,2}$ consisting of all the orthogonal 2-frames with o as the origin.

The function $T\colon X_d\to X_d$ defined by $T(x_1,x_2,x_3)=(x_2,x_3,x_1)$ is a periodical transformation of period 3 and has no fixed point.

Let p be a point of S^{n+1} and let S^n be the n-sphere contained in S^{n+1} consisting of all the points x with $\rho(p,x)=\cos^{-1}((1+2\cos d)/3)^{\frac{1}{2}}$. It is easily seen that every d-triple (x_1,x_2,x_3) on S^{n+1} with $\rho(p,x_1)=\rho(p,x_2)=\rho(p,x_3)$ is a $(2\pi/3)$-triple on S^n and conversely every $(2\pi/3)$-triple on S^n is a d-triple on S^{n+1}. Hence all the $(2\pi/3)$-triples on S^n form a subset A_p of X_d. The set A_p is homeomorphic to the Stiefel manifold $V_{n+1,2}$ and is invariant under the periodical transformation T. For $n>1$, A_p is con-

nected; but for $n=1$, A_p consists of two components each of which is homeomorphic to a circle and is invariant under T.

Let I be the unit closed interval $[0,1]$. Then a map $h\colon A_p\times I\to X_d$ can be constructed as follows. Given any $(x_1,x_2,x_3)\in A_p$ we let Π be the n-plane perpendicular to the 2-plane $[opx_1]$ at o. Let (px_1) be the geodesic on S^{n+1} joining p and x_1, i.e., the shorter arc of the great circle $S^{n+1}\cap[opx_1]$ with end points p, x_1. For each $t\in I$ we denote by σ_t the rotation of S^{n+1} around Π such that $\sigma_t(x_1)$ is the point of (px_1) with $\rho(x_1,\sigma_t(x_1))=t\rho(p,x_1)$. Now we define $h\colon A_p\times I\to X_d$ by $h((x_1,x_2,x_3),t)=(\sigma_t(x_1),\sigma_t(x_2),\sigma_t(x_3))$. Clearly h is a homeomorphism of $A_p\times I$ into X_d, $h(A_p\times 0)=A_p$ and $B_p=h(A_p\times 1)$ consists of all the d-triples (x_1,x_2,x_3) on S^{n+1} with $x_1=p$.

3. Proof of Theorem 1. Suppose that Theorem 1 is false, i.e., there is a map f of S^{n+1} into R^n and a number d, $0<d<2\pi/3$, such that for no $(x_1,x_2,x_3)\in X_d$, $f(x_1)=f(x_2)=f(x_3)$. Then a map g of X_d into a $(2n-1)$-sphere S^{2n-1} can be constructed as follows. For any $(x_1,x_2,x_3)\in X_d$ we let

$$f(x_1)=(\alpha_1,\cdots,\alpha_n),\quad f(x_2)=(\alpha_{n+1},\cdots,\alpha_{2n}),\quad f(x_3)=(\alpha_{2n+1},\cdots,\alpha_{3n});$$

$$\beta_i=\alpha_i-(\alpha_i+\alpha_{n+i}+\alpha_{2n+i})/3,$$

$$\beta_{n+i}=\alpha_{n+i}-(\alpha_i+\alpha_{n+i}+\alpha_{2n+i})/3\qquad \beta_{2n+i}=\alpha_{2n+i}-(\alpha_i+\alpha_{n+i}+\alpha_{2n+i})/3,$$
$$i=1,\cdots,n;$$

$$\gamma_i=\beta_i/(\sum_{k=1}^{3n}\beta_k{}^2)^{\frac12},\qquad i=1,\cdots,3n.$$

Notice that our assumption implies that $\alpha_i=\alpha_{n+i}=\alpha_{2n+i}$ does not hold for all $i=1,\cdots,n$. Therefore $\sum_{k=1}^{3n}\beta_k{}^2>0$ and hence γ are well-defined. Let S^{2n-1} be the $(2n-1)$-sphere in R^{3n} given by

$$u_1{}^2+\cdots+u_{3n}{}^2=1,\qquad u_i+u_{n+i}+u_{2n+i}=0,\qquad i=1,\cdots,n,$$

where $u_1,\cdots,u_{3n}$ are coordinates of points in R^{3n}. Then $g(x_1,x_2,x_3)=(\gamma_1,\cdots,\gamma_{3n})$ gives a map g of X_d into S^{2n-1}.

The map $T\colon S^{2n-1}\to S^{2n-1}$ defined by

$$T(u_1,\cdots,u_n,u_{n+1},\cdots,u_{3n})=(u_{n+1},\cdots,u_{3n},u_1,\cdots,u_n)$$

is a periodical transformation of period 3 and has no fixed point. Moreover $gT=Tg$.

Let p be a point of S^{n+1} where the first coordinate of $f(p)$ attains its least upper bound. Let A_p and B_p be as in the preceding section. Then for any $(x_1, x_2, x_3) \in B_p$, $g(x_1, x_2, x_3) = (\gamma_1, \cdots, \gamma_{3n})$ must satisfy $\gamma_1 \geqq \gamma_{n+1}$. Therefore $g(B_p)$ is a proper subset of S^{2n-1} and hence $g|B_p$, i. e., the map g restricted on B_p, is inessential. As seen in the preceding section, A_p and B_p may be regarded as bases of a cylinder contained in X_d. Hence, if we can show that $g|A_p$ is essential, we arrive at a contradiction which completes the proof of Theorem 1.

4. Special homology theory. In order to prove that $g|A_p$ is essential, we need the following special case of the special homology theory of Smith. Let X be a compact Hausdorff space and let T be a periodical transformation of X which is of period 3 and has no fixed point. Let ρ, ρ' stand for $1 - T$, $1 + T + T^2$ or vice versa. As seen in [6], we have, for each integer $k \geqq 0$, a (Čech) homology group $H_k(X)$ and two special homology groups $H_k{}^\rho(X)$ and $H_k{}^{\rho'}(X)$, where the group Z_3 of integers mod 3 is used as coefficient group. We also have homomorphisms

$$\partial\colon H_{k+1}{}^\rho(X) \to H_k{}^{\rho'}(X), \quad i\colon H_k{}^{\rho'}(X) \to H_k(X), \quad j\colon H_k(X) \to H_k{}^\rho(X).$$

(4.1) *Let X, T, ∂, i, j be as above. Then the sequence*

$$H_0{}^\rho(X) \xleftarrow{j} H_0(X) \xleftarrow{i} H_0{}^{\rho'}(X) \xleftarrow{\partial} \cdots$$

$$\longleftarrow H_{k-1}{}^{\rho'}(X) \xleftarrow{\partial} H_k{}^\rho(X) \xleftarrow{j} H_k(X) \xleftarrow{i} H_k{}^{\rho'}(X) \xleftarrow{\partial} H_{k+1}{}^\rho(X) \longleftarrow \cdots$$

is exact. [6]

(4.2) *Let X, T, ∂, i, j be as above and let Y, T, ∂, i, j be their analogies. Then for any map $g\colon X \to Y$ with $gT = Tg$ there are induced homomorphisms*

$$g\colon H_k(X) \to H_k(X), \quad g\colon H_k{}^\rho(X) \to H_k{}^\rho(X), \quad g\colon H_k{}^{\rho'}(X) \to H_k{}^{\rho'}(X)$$

such that the diagram

$$\begin{tikzcd} H_k{}^\rho(X) \arrow[d, "g"] & H_k(X) \arrow[l, "j"'] \arrow[d, "g"] & H_k{}^{\rho'}(X) \arrow[l, "i"'] \arrow[d, "g"] & H_{k+1}{}^\rho(X) \arrow[l, "\partial"'] \arrow[d, "g"] \\ H_k{}^\rho(Y) & H_k(Y) \arrow[l, "j"'] & H_k{}^{\rho'}(Y) \arrow[l, "i"'] & H_{k+1}{}^\rho(Y) \arrow[l, "\partial"'] \end{tikzcd}$$

is commutative. [6]

As a consequence of (4.1) we have:

(4.3) *Let X, T, ∂, i, j be as above. If for some integer $m > 0$, $H_k(X)$ is equal to Z_2 or 0 according as $k = 0$, m or not, then $H_k{}^{\rho}(X) = 0$ or Z_2 according as $k > m$ or not. Moreover $i\colon H_m{}^{\rho'}(X) \to H_m(X)$, $j\colon H_0(X) \to H_0{}^{\rho}(X)$ and $\partial\colon H_{k+1}{}^{\rho}(X) \to H_k{}^{\rho'}(X)$, $k = 0, \cdots, m-1$, are isomorphisms onto.* [6]

5. Continuation of the proof of Theorem 1. Now we return to the proof of Theorem 1 and assert that $g|A_p$ is essential. Since the homomorphism of homology groups induced by an inessential map is always trivial, we have only to prove

(5.1) *The homomorphism $g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$ induced by the map $g|A_p$ is not trivial.*

Suppose that n is even. Then $H_k(A_p)$ is the same as $H_k(S^{2n-1})$ which is equal to Z_2 or 0 according as $k = 0$, $2n-1$ or not [7]. By (4.3), all the horizontal homomorphisms in the diagram

$$\begin{tikzcd}
H_0(A_p) \arrow[r, "j"] \arrow[d, "g"] & H_0{}^{\rho}(A_p) \arrow[d, "g"] & H_1{}^{\rho'}(A_p) \arrow[l, "\partial"'] \arrow[d, "g"] & H_2{}^{\rho}(A_p) \arrow[l, "\partial"'] \arrow[d, "g"] \\
H_0(S^{2n-1}) \arrow[r, "j"] & H_0{}^{\rho}(S^{2n-1}) & H_1{}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] & H_2{}^{\rho}(S^{2n-1}) \arrow[l, "\partial"']
\end{tikzcd}$$

$$\begin{tikzcd}
{} & \cdots \arrow[l, "\partial"'] & H_{2n-1}{}^{\rho}(A_p) \arrow[l, "\partial"'] \arrow[r, "i"] \arrow[d, "g"] & H_{2n-1}(A_p) \arrow[d, "g"] \\
{} & \cdots \arrow[l, "\partial"'] & H_{2n-1}{}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] \arrow[r, "i"] & H_{2n-1}(S^{2n-1})
\end{tikzcd}$$

are isomorphisms onto. Since A_p and S^{2n-1} are both connected, $g\colon H_0(A_p) \to H_0(S^{2n-1})$ is an isomorphism onto. Hence, by (4.2), all the vertical homomorphisms are isomorphisms onto. In particular,

$$g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$$

is not trivial.

Suppose that $n = 1$. Then A_p consists of two components and each of the components is topologically a circle invariant under T. It is easily seen that the proof above remains true when A_p is replaced by either of its components. Hence for $n = 1$, $g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$ is also not trivial. Notice that this is essentially the proof in [3].

Suppose now that n is an odd number > 1. Since A_p consists of all the $(2\pi/3)$-triples on S^n, it contains a subset A_p' consisting of all the $(2\pi/3)$-triples on an $(n-1)$-sphere S^{n-1}. As seen in Section 2, A_p' is homeomorphic to the Stiefel manifold $V_{n,2}$ and therefore $H_k(A_p')$ is equal to Z_3 or 0 according as $k = 0,\ 2n-3$ or not. Therefore in the diagram

$$\begin{tikzcd}
H_0(A_p') \arrow[r, "j"] \arrow[d] & H_0{}^{\rho}(A_p') \arrow[d] & H_1{}^{\rho'}(A_p') \arrow[l, "\partial"'] \arrow[d] & \cdots \arrow[l, "\partial"'] & H_{2n-3}{}^{\rho'}(A_p') \arrow[l, "\partial"'] \arrow[d] \\
H_0(S^{2n-1}) \arrow[r, "j"] & H_0{}^{\rho}(S^{2n-1}) & H_1{}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] & \cdots \arrow[l, "\partial"'] & H_{2n-3}{}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"']
\end{tikzcd}$$

all the horizontal homomorphisms are isomorphisms onto and among the vertical homomorphisms which are induced by the map $g|A_p'$, the first one on the left is an isomorphism onto. Hence, by (4.3), all the vertical homomorphisms are isomorphisms onto. Let I be the image of $H_{2n-3}{}^{\rho'}(A_p')$ in $H_{2n-3}{}^{\rho'}(A_p)$ under the homomorphism induced by the inclusion map. Then g maps I isomorphically onto $H_{2n-3}{}^{\rho}(S^{2n-1})$.

If $n > 3$, it is known [7] that $H_{2n-3}(A_p)$ and $H_{2n-2}(A_p)$ are both 0. Therefore, by (4.1), $\partial\colon H_{2n-2}{}^{\rho}(A_p) \to H_{2n-3}{}^{\rho'}(A_p)$ is an isomorphism onto and hence

$$I \subset \partial H_{2n-2}{}^{\rho}(A_p). \tag{5.2}$$

If $n = 3$, A_p is a sphere bundle over S^3 with respect to the projection $(x_1, x_2, x_3) \to x_1$. Since the projection induces an isomorphism of $H_3(A_p)$ onto $H_3(S^3)$ and maps A_p' into S^2, it follows that $i\colon H_3{}^{\rho'}(A_p) \to H_3(A_p)$ maps I into 0. Hence (5.2) also holds for $n = 3$.

Now we observe the diagram

$$\begin{tikzcd}
 & H_{2n-2}{}^{\rho}(A_p) \arrow[dl, "g\partial"'] \arrow[d, "g"] & H_{2n-1}{}^{\rho'}(A_p) \arrow[l, "\partial"'] \arrow[r, "i"] \arrow[d, "g"] & H_{2n-1}(A_p) \arrow[d, "g"] \\
H_{2n-3}{}^{\rho'}(S^{2n-1}) & H_{2n-2}{}^{\rho}(S^{2n-1}) \arrow[l, "\partial"'] & H_{2n-1}{}^{\rho'}(S^{2n-1}) \arrow[l, "\partial"'] \arrow[r, "i"] & H_{2n-1}(S^{2n-1})
\end{tikzcd}$$

It is easily seen that $i\colon H_{2n-1}{}^{\rho'}(A_p) \to H_{2n-1}(A_p)$ is an isomorphism onto. Since $n \geqq 3$, $H_{2n-2}(A_p) = 0$. It follows from (4.1) that $\partial\colon H_{2n-1}{}^{\rho'}(A_p) \to H_{2n-2}{}^{\rho}(A_p)$ is an isomorphism onto. Since, by (4.3), all the homomorphisms of the lower row are isomorphisms and since

$$g\partial H_{2n-2}{}^{\rho'}(A_p) \supset gI \neq 0,$$

we infer from (4.2) that $g\colon H_{2n-1}(A_p) \to H_{2n-1}(S^{2n-1})$ is not trivial. This completes the proof of (5.1) and hence Theorem 1 is proved.

6. A generalization. As in [2], Theorem 1 can be extended to a theorem on compact Riemannian manifolds without singularity.

Let M be a Riemannian manifold without singularity. For any point a of M and any unit tangent vector v at a there is a geodesic beginning at a and tangent to v. We shall denote by (a, v, e) the point of M obtained by moving a point along the geodesic a distance e from a.

THEOREM 2. *Let M be a compact $(n+1)$-dimensional Riemannian manifold without singularity and let f be a map of M into the euclidean n-space. Then for any $e > 0$ there exists a point a of M and three unit tangent vectors v_1, v_2, v_3 of M at a such that the angle between any two of v_1, v_2, v_3 is equal to $2\pi/3$ and $f(a, v_1, e) = f(a, v_2, e) = f(a, v_3, e)$.*

The proof of Theorem 2 is the same as that of Theorem 1 except for a few modifications. Let V be the totality of (a, v_1, v_2, v_3), where a is a point of M and v_1, v_2, v_3 are unit tangent vectors at a such that the angle between any two of them is equal to $2\pi/3$. If Theorem 2 is false, then there is a map $f\colon M \to R^n$ and a number $e > 0$ such that for no $(a, v_1, v_2, v_3) \in V$, $f(a, v_1, e) = f(a, v_2, e) = f(a, v_3, e)$. Therefore we may construct a map $g\colon V \to S^{2n-1}$ as in the proof of Theorem 1. Since M is compact, there is a point p of M where the first coordinate of $f(p)$ attains its least upper bound. Let A_p be the subset of V consisting of all the elements (a, v_1, v_2, v_3) with $a = p$. As (5.1), the map $g \mid A_p$ is essential. For any $(a, v_1, v_2, v_3) \in A_p$ and $t \in I$ we define $(a(t), v_1(t), v_2(t), v_3(t)) \in V$ such that $a(t) = (p, -v_1, te)$ and $v_1(t)$, $v_2(t)$, $v_3(t)$ are parallel displacements of v_1, v_2, v_3 along the geodesic $a(s)$, $0 \leqq s \leqq t$. Then

$$((a, v_1, v_2, v_3), t) \to (a(t), v_1(t), v_2(t), v_3(t))$$

defines a map h of $A_p \times I$ into V with

$$h((a, v_1, v_2, v_3), 0) = (a, v_1, v_2, v_3).$$

Since $h(A_p \times 1)$ consists of all the elements (a, v_1, v_2, v_3) with $p = (a, v_1, e)$, it follows that the map g restricted on $B_p = h(A_p \times 1)$ is inessential. Hence we arrive at a contradiction.

Theorem 2 is a generalization of Theorem 1, because the former becomes the latter if M is an $(n+1)$-sphere with the spherical distance function as its Riemannian metric and $e = \cos^{-1}((1 + 2\cos d)/3)^{\frac{1}{2}}$.

UNIVERSITY OF PENNSYLVANIA.

REFERENCES.

[1] B. Knaster, *Colloquium Mathematicum*, vol. 1 (1947), pp. 30-31.

[2] H. Hopf, "Verallgemeinerung bekannter Abildungs- und Überdeckungssätze," *Portugaliae Mathematica*, vol. 4 (1944), pp. 129-139.

[3] S. Kakutani, "A proof that there exists a circumscribing cube around any bounded closed convex set in R^3," *Annals of Mathematics*, vol. 43 (1942), pp. 739-741..

[4] H. Yamabe and Z. Yujobô, "On the continuous functions defined on a sphere," *Osaka Mathematical Journal*, vol. 2 (1950), pp. 19-22.

[5] E. E. Floyd, "Real-valued mappings of spheres," *Proceedings of the American Mathematical Society*, vol. 6 (1955), pp. 957-959.

[6] ———, "On periodic maps and the Euler characteristics of associated spaces," *Transactions of the American Mathematical Society*, vol. 72 (1952), pp. 138-147.

[7] E. Stiefel, "Richtungsfelder und Fernparallelismus in n-dimensionalen Mannigfaltigkeiten," *Commentarii Mathematici Helvetici*, vol. 8 (1936), pp. 3-51.

A FORMULA FOR SEMISIMPLE LIE GROUPS.*

By HARISH-CHANDRA.

1. Introduction. Let G be a connected semisimple Lie group and $\mathcal{E}$ the set of all equivalence classes of irreducible unitary representations of G. Let T_ω denote the character of any class $\omega \in \mathcal{E}$ (see [4(a)]). Then the Plancherel formula for G is equivalent to the following statement. *There exists a unique positive measure $d\omega$ on $\mathcal{E}$ (called the Plancherel measure) such that*

$$f(1) = \int_{\mathcal{E}} T_\omega(f)\, d\omega$$

for all[1] $f \in C_c^\infty(G)$. Let δ denote the Dirac measure on G corresponding to the unit mass at 1 so that $\delta(f) = f(1)$. Then the above formula may also be interpreted in the form

$$\delta = \int_{\mathcal{E}} T_\omega d\omega.$$

Let T be a distribution and D a differential operator on G. Then, for any $x, y \in G$, we define the distribution $T' = xTy$ and the differential operator $D' = xDy$ as follows. $T'(f) = T(f')$ and $D'f = Df'$ $(f \in C_c^\infty(G))$, where $f'(z) = f(xzy)$ $(z \in G)$. Also, put $xT = xTy$, $Tx = yTx$, for $y = 1$. T is called invariant if $xTx^{-1} = T$ for all $x \in G$. Let $\mathfrak{Z}$ be the algebra of those differential operators D for which $D = xDy$ $(x, y \in G)$. We say that T is an eigen-distribution of $\mathfrak{Z}$ if it is an eigen-distribution for every D in $\mathfrak{Z}$. Let Z be the center of G. Then T is an eigen-distribution of Z if zT is a numerical multiple of T for every $z \in Z$. It is known (see[4(a)]) that the characters T_ω $(\omega \in \mathcal{E})$ are invariant and that they are eigen-distributions of both $\mathfrak{Z}$ and Z. Hence the Plancherel formula may be regarded as an "expansion" of δ in terms of such invariant eigen-distributions.

Although the existence and uniqueness of the Plancherel measure are known, so far no general method of computing it has been found. The object of this paper is to give a formula which can be regarded as a first step towards the determination of $d\omega$. Let G' and S, respectively, denote the sets

* Received December 4, 1956.

[1] See footnote 1 of [4(g)] for certain notational conventions.

of regular and singular elements in G (see [4(c)]). Consider a Cartan subgroup A of G and let $\mathfrak{H}$ denote the algebra of those differential operators on A which are invariant under all translations of A. Then for any $f \in C_c^\infty(G)$, we shall define a function Ψ_f on $A' = A \cap G'$ of class C^∞ in such a way that the following conditions hold.[2]

(1) If $f' = xfx^{-1}$ $(x \in G, f \in C_c^\infty(G))$, then $\Psi_f = \Psi_{f'}$.

(2) There exists a homomorphism γ of $\mathfrak{Z}$ into $\mathfrak{H}$ such that $\Psi_{zf} = \gamma(z)\Psi_f$ for all $z \in \mathfrak{Z}$ and $f \in C_c^\infty(G)$.

(3) For every $u \in \mathfrak{H}$ and $f \in C_c^\infty(G)$, $u\Psi_f$ remains bounded on A' and Ψ_f vanishes outside some compact subset of A.

(4) The mapping $f \rightarrow \Psi_f$ is continuous in a suitable sense (see Theorem 2).

Let l be the rank of G. Then $A \cap S$ is the union of a finite number of closed subgroups of A of dimension $l-1$. (3) implies that $u\Psi_f$ has no singularities (on A) except possible jumps across $A \cap S$. Let $\hat{A}$ be the character group of A and $T_{\hat{a}}(f)$ the value of the Fourier transform of Ψ_f at $\hat{a} \in \hat{A}$. Then it follows from (1) and (4) that $T_{\hat{a}}$ is an invariant distribution on G (see Lemma 17). Moreover, since $Z \subset A$, it is clear that $T_{\hat{a}}$ is an eigen-distribution of Z. For any function $\phi \in C_c^\infty(A)$, let $\tilde{\phi}$ denote the Fourier transform of ϕ. Then it is clear that, for any $u \in \mathfrak{H}$, there exists an analytic function $\hat{u}$ on $\hat{A}$ such that $(u\phi)^\sim = \hat{u}\tilde{\phi}$ $(\phi \in C_c^\infty(A))$. Let $\chi_{\hat{a}}(z)$ $(z \in \mathfrak{Z}, \hat{a} \in \hat{A})$ denote the value of $(\gamma(z))^\wedge$ at $\hat{a}$. Then if Ψ_f could be extended to a function of class C^∞ on A, it would follow from (2) that

$$T_{\hat{a}}(zf) = \chi_{\hat{a}}(z)\, T_{\hat{a}}(f).$$

Hence except for the above-mentioned jumps, $T_{\hat{a}}$ would have been an eigen-distribution of $\mathfrak{Z}$.

Let $l_-(A)$ denote the dimension of the maximal compact subgroup of A/Z. We say that A is fundamental if $l_-(A)$ has the maximum possible value. If A is fundamental, we can select an open neighborhood B of 1 in A and a connected component A_1 of $B \cap A'$ such that 1 lies in the closure of A_1 and the following additional condition holds.

(5) There exists an element $u_0 \in \mathfrak{H}$ such that

$$f(1) = \lim_{a \rightarrow 1} (u_0\Psi_f)(a) \qquad (a \in A_1) \tag{I}$$

for all $f \in C_c^\infty(G)$.

[2] $\Psi_f = \epsilon_+ F_f \prod_{\alpha \in P} |\eta_\alpha|^{\frac{1}{2}}$ in the notation of Lemma 18.

Let us agree, for a moment, to ignore the complications due to the jumps. Then (5) implies the formula

$$\text{(II)} \qquad f(1) = \int_{\hat{A}} \hat{u}_0(\hat{a}) T_{\hat{a}}(f)\, d\hat{a} \qquad (f \in C_c^\infty(G)),$$

where $d\hat{a}$ is the (suitably normalized) Haar measure on $\hat{A}$. Therefore

$$\delta = \int_{\hat{A}} \hat{u}_0(\hat{a}) T_{\hat{a}}\, d\hat{a},$$

and since $T_{\hat{a}}$ are invariant eigen-distributions of Z and $\mathfrak{Z}$, we should expect this formula to be closely related to the Plancherel formula.

Let $r(G)$ be the maximum number of nonconjugate Cartan subgroups of G. In case $r(G) = 1$, it is actually true that Ψ_f can be extended to a function of class C^∞ on A for every $f \in C_c^\infty(G)$. Hence the above formula holds in this case. Moreover, it is then possible to define a mapping $\hat{a} \to \omega(\hat{a})$ of $\hat{A}$ into $\mathcal{E}$ such that $T_{\hat{a}} = cT_{\omega(\hat{a})}$, where c is a constant. Then

$$\delta = c \int_{\hat{A}} \hat{u}_0(\hat{a}) T_{\omega(\hat{a})} d\hat{a}$$

and, in fact this is substantially the same as the Plancherel formula for G. Thus if $r(G) = 1$, the problem of the determination of the Plancherel measure is solved completely. This is so in particular if G is either compact or complex (see [4(b)]).

Now in the general case $(r(G) > 1)$, the jumps of the function Ψ_f (or its derivatives) cannot be ignored, and therefore $T_{\hat{a}}$ is no longer an eigen-distribution of $\mathfrak{Z}$. Nevertheless, there are good reasons to believe (see [4(c)]) that for suitable $\hat{a} \in \hat{A}$, $T_{\hat{a}}$ is intimately related to a character T_ω of G. Hence equation (I) may still be regarded as a first step towards the derivation of the Plancherel formula. The importance of such a relation has been clearly recognized by Gelfand and Graev [3].

Now suppose for a moment that A is compact so that $\hat{A}$ is discrete. In view of equation (II) (which, however, is not quite exact due to the jumps of Ψ_f), one would expect to get a "discrete series" (see [4(f)]) in $\mathcal{E}$ parametrized by $\hat{A}$. More precisely, we should expect the existence of a mapping which assigns to each $\hat{a}$ lying in a suitable subset $\hat{A}_0$ of $\hat{A}$, a discrete class $\omega(\hat{a})$ in $\mathcal{E}$ such that the Plancherel measure of $\omega(\hat{a})$ is $c\hat{u}_0(\hat{a})$, where c is a constant independent of $\hat{a}$. This expectation has actually been confirmed in a large number of cases (see [4(f)]).

If G is simple, its first Betti number $b(G)$ is either 0 or 1. Assuming that A is compact, we should expect to get a discrete series in both cases.

So far, a general method for constructing a discrete series has been obtained only when $b(G)=1$ (see [4(d), (e), (f)]).

This paper is divided into two parts. The main results of Part I are contained in Theorem I and the Corollary to Lemma 12. We need them in Part II in order to carry over the results of [4(h), (i)] from its Lie algebra to the group G itself. Sections 4 and 5 are devoted to the verification of the five conditions stated above. A short account of the principal results of this paper has appeared in [4(j)].

Part I.

2. Proof of Theorem 1. Let R and C be the fields of real and complex numbers, respectively, and let G be a connected semisimple Lie group with the Lie algebra $\mathfrak{g}_0$ over R. Let $\mathfrak{h}_0$ be a Cartan subalgebra of $\mathfrak{g}_0$ and A the corresponding Cartan subgroup of G (see [4(c), § 2]). Our main object in this section is to prove the following theorem.

THEORM 1. *Let a_0 be an element in A and Ξ the centralizer of a_0 in G. Denote the natural mapping of G on the factor space $G^*=G/\Xi$ by $x \rightarrow x^*$ $(x \in G)$. Then we can find a neighborhood B of a_0 in A with the following property. Given any compact set ω in G, there exists a compact set Ω^* in G^* satisfying the condition that, if $xax^{-1} \in \omega$ for some $a \in B$ and $x \in G$, then $x^* \in \Omega^*$.*

The proof is rather long and requires considerable preparation. First we need two results on nilpotent groups. Let F be a field which is either R or C, and let N be a connected Lie group and $\mathfrak{n}$ its Lie algebra over F. (If $F=C$, we assume of course that N is a complex analytic group.) Suppose $\mathfrak{n}$ is nilpotent and $\mathfrak{n}^{(k)}$ $(k=1,2,\cdots)$ are ideals in $\mathfrak{n}$ such that $\mathfrak{n}^{(1)}=\mathfrak{n}$, $[\mathfrak{n},\mathfrak{n}^{(k)}] \subset \mathfrak{n}^{(k+1)}$ $(k \geqq 1)$ and $\mathfrak{n}^{(k)}=\{0\}$ if k is sufficiently large. Furthermore suppose $\mathfrak{n}$ can be written as a direct sum of two subspaces $\mathfrak{n}_1$, $\mathfrak{n}_2$ satisfying the following two conditions:

(1) $\mathfrak{n}_1$ is a subalgebra of $\mathfrak{n}$,

(2) $\mathfrak{n}^{(k)}=\mathfrak{n}_1 \cap \mathfrak{n}^{(k)}+\mathfrak{n}_2 \cap \mathfrak{n}^{(k)}$ for all $k \geqq 1$.

Then we have the following result.

LEMMA 1. *Under the above conditions every element in N can be written in the form* $\exp X_2 \exp X_1$, *where $X_1 \in \mathfrak{n}_1$ and $X_2 \in \mathfrak{n}_2$.*

Without loss of generality, we may assume that N is simply connected. Then $\mathfrak{n}$ being nilpotent, the exponential mapping is a one-one regular mapping of $\mathfrak{n}$ onto N. We denote its inverse by $x \to \log x$ $(x \in N)$. X being any element in N, we shall first show that for every integer $k \geqq 0$, we can find $X_1 \in \mathfrak{n}_1$ such that

$$\log(\exp X \exp(-X_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k+1)}.$$

We use induction on k. If $k = 0$ our assertion is true trivially. So let us suppose $k \geqq 1$. By the induction hypothesis, we can choose $Y_1 \in \mathfrak{n}_1$ such that $Z = \log(\exp X \exp(-Y_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k)}$. Select $Z' \in \mathfrak{n}^{(k)}$ such that $Z - Z' \in \mathfrak{n}_2$. Then $Z' = Z_1 + Z_2$, where $Z_i \in \mathfrak{n}_i \cap \mathfrak{n}^{(k)}$ $(i = 1, 2)$. Hence, by the Campbell-Hausdorff formula, we get

$$\log(\exp Z \exp(-Z_1)) \equiv Z - Z_1 \bmod \mathfrak{n}^{(k+1)}.$$

Moreover, $Z - Z_1 = (Z - Z') + Z_2 \in \mathfrak{n}_2$, and therefore

$$\log(\exp X \exp(-Y_1)\exp(-Z_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k+1)}.$$

However, $\mathfrak{n}_1$ is a nilpotent algebra, and therefore $\exp Z_1 \exp Y_1 = \exp X_1$ for some $X_1 \in \mathfrak{n}_1$. Hence $\log(\exp X \exp(-X_1)) \in \mathfrak{n}_2 + \mathfrak{n}^{(k+1)}$.

Now taking k sufficiently large, we get $X_2 = \log(\exp X \exp(-X_1)) \in \mathfrak{n}_2$, and so $\exp X = \exp X_2 \exp X_1$. This proves the lemma.

Let $X_1, \cdots, X_r$ be a base for $\mathfrak{n}$ over F such that $[X_i, X_j] \in \sum_{k>j} FX_k$ $(1 \leqq i \leqq j \leqq r)$. Put $\mathfrak{n}_{(0)} = \{0\}$, $\mathfrak{n}_{(j)} = \sum_{1 \leqq i \leqq j} FX_i$ $(1 \leqq j \leqq r)$, and let π_j denote the projection of $\mathfrak{n}$ on $\mathfrak{n}_{(j)}$ given by $\pi_j X_i = X_i$ $(1 \leqq i \leqq j)$ and $\pi_j X_i = 0$ $(j < i \leqq r)$. Let ${}_m\mathfrak{n}_{(j)}$ denote the Cartesian product of $\mathfrak{n}_{(j)}$ with itself m times.

LEMMA 2. *Suppose N is simply connected and m is a positive integer. Then for each j $(1 \leqq j \leqq r)$, there exists a polynomial mapping*[3] *p_j of ${}_m\mathfrak{n}_{(j-1)}$ into $\mathfrak{n}_{(j)}$ such that*

$$\pi_j \log(\exp Y_1 \exp Y_2 \cdots \exp Y_m)$$
$$= \pi_j(Y_1 + \cdots + Y_m) + p_j(\pi_{j-1}Y_1, \pi_{j-1}Y_2, \cdots, \pi_{j-1}Y_m)$$

for all $Y_1, \cdots, Y_m \in \mathfrak{n}$.

We shall prove this by induction on $r = \dim \mathfrak{n}$. If $r = 1$, $\mathfrak{n}$ is abelian

[3] Let U, V be two vector spaces over F of finite dimension. A mapping p of U into V is called a polynomial mapping if, for every linear function λ on V, the function $u \to \lambda(p(u))$ $(u \in U)$ is a polynomial function on U.

and our statement is obvious. So now suppose $r \geqq 2$. Put $\mathfrak{n}^* = \mathfrak{n}/FX_r$ and $N^* = N/N_r$, where N_r is the one-parameter subgroup of N corresponding to X_r. Since X_r lies in the center of $\mathfrak{n}$, it is clear that $\log(\exp X \exp Y) = X + Y$ $(X \in \mathfrak{n}, Y \in FX_r)$, and therefore the exponential mapping of $\mathfrak{n}^*$ onto N^* is still one-one. Let $X \to X^*$ $(X \in \mathfrak{n})$ denote the natural mapping of $\mathfrak{n}$ on $\mathfrak{n}^*$, and let $\mathfrak{n}_{(j)}{}^*$ be the image of $\mathfrak{n}_{(j)}$ $(1 \leqq j \leqq r)$ under this mapping. Define the projection $\pi_j{}^*$ of $\mathfrak{n}^*$ on $\mathfrak{n}_{(j)}{}^*$ by $\pi_j{}^* X^* = (\pi_j X)^*$ $(X \in \mathfrak{n}, 1 \leqq j \leqq r)$. Then since $\dim \mathfrak{n}^* < \dim \mathfrak{n}$, our induction hypothesis is applicable to $\mathfrak{n}^*$. Hence for each j, there exists a polynomial mapping q_j of ${}_m\mathfrak{n}_{(j-1)}$ into $\mathfrak{n}_j$ such that

$$\pi_j \log(\exp Y_1 \cdots \exp Y_m)$$
$$\equiv \pi_j(Y_1 + \cdots + Y_m) + q_j(\pi_{j-1}Y_1, \cdots, \pi_{j-1}Y_m) \bmod FX_r$$

for $Y_1, \cdots, Y_m \in \mathfrak{n}$. But if $j < r$, $\mathfrak{n}_{(j)} \cap (FX_r) = \{0\}$, and therefore

$$\pi_j \log(\exp Y_1 \cdots \exp Y_m) = \pi_j(Y_1 + \cdots + Y_m) + q_j(\pi_{j-1}Y_1, \cdots, \pi_{j-1}Y_m).$$

On the other hand, if $j = r$, π_r is the identity mapping of $\mathfrak{n}$. Moreover, it is known that $(Y_1, \cdots, Y_m) \to \log(\exp Y_1 \cdots \exp Y_m)$ is a polynomial mapping of ${}_m\mathfrak{n} = {}_m\mathfrak{n}_{(r)}$ into $\mathfrak{n}$ (see Birkhoff [1]). Now put

$$p_r(Y_1, \cdots, Y_m) = \log(\exp Y_1 \cdots \exp Y_m) - (Y_1 + \cdots + Y_m).$$

Then since X_r belongs to the center of $\mathfrak{n}$, it is clear that $p_r(Y_1, \cdots, Y_m) = p_r(\pi_{r-1}Y_1, \cdots, \pi_{r-1}Y_m)$. Hence

$$\log(\exp Y_1 \cdots \exp Y_m) = (Y_1 + \cdots + Y_m) + p_r(\pi_{r-1}Y_1, \cdots, \pi_{r-1}Y_m),$$

and this proves our assertion for $j = r$.

Let $\mathfrak{g}$, $\mathfrak{h}$ be the complexifications of $\mathfrak{g}_0$, $\mathfrak{h}_0$, respectively, and let G_c be a complex analytic group with the Lie algebra $\mathfrak{g}$. From now on we shall use the notation of [4(g), (h)] without further comment. In view of the Corollary of Lemma 1 of [4(c)], we may obviously assume that $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$. For each root α (of $\mathfrak{g}$ with respect to $\mathfrak{h}$), select an eleemnt $X_\alpha \neq 0$ in $\mathfrak{g}$ such that $[H, X_\alpha] = \alpha(H) X_\alpha$ for all $H \in \mathfrak{h}$. Define the set P of positive roots as in [4(h), § 5], and put $\mathfrak{n} = \sum_{\alpha \in P} CX_\alpha$. Let A_c be the analytic subgroup of G_c corresponding to $\mathfrak{h}$. If α is a root, we denote by ξ_α the corresponding character of A_c so that $\xi_\alpha(\exp H) = e^{\alpha(H)}$ $(H \in \mathfrak{h})$. Let a_0 be a fixed element in A_c and P_1 the subset of those roots $\alpha \in P$ for which $\xi_\alpha(a_0) = 1$. Then if P_2

is the complement of P_1 on P, we put $\mathfrak{n}_1 = \sum_{\alpha \in P_1} CX_\alpha$, $\mathfrak{n}_2 = \sum_{\alpha \in P_2} CX_\alpha$. Let $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ be all the roots in P. Put

$$\mathfrak{n}^{(k)} = \sum_{k \leqq i \leqq r} CX_{\alpha_i} \qquad (k \geqq 1).$$

Then it is obvious that all the conditions of Lemma 1 are fulfilled. Let N_c and N_1 be the (complex) analytic subgroups of G_c corresponding to $\mathfrak{n}$ and $\mathfrak{n}_1$, respectively. Also, let N_2 denote the set of all elements in N_c of the form $\exp X$ $(X \in \mathfrak{n}_2)$. It is well known that N_c is simply connected, and therefore the exponential mapping defines an isomorphism of the complex vector space $\mathfrak{n}$ onto N_c (with respect to its structure as a complex manifold). Hence N_2 is closed in N_c.

Choose a compact neighborhood B_c of a_0 in A_c such that, if $\alpha \in P_2$, then ξ_α never takes the value 1 on B_c.

LEMMA 3. *Let Ξ_c denote the centralizer of a_0 in G_c and $x \to x^*$ the natural mapping of G_c onto $G_c^* = G_c/\Xi_c$. Then for any compact set ω_c in G_c, we can select a compact set Ω_c^* in G_c^* satisfying the following condition. If $xax^{-1} \in \omega_c$ for some $x \in G_c$ and $a \in B_c$, then $x^* \in \Omega_c^*$.*

We shall derive Theorem 1 from the above lemma. But in order to prove this lemma, we need some additional facts.

LEMMA 4. *There exist compact sets ω_1, ω_2 in N_1, N_2, respectively, having the following property. Suppose $n_2 a n_1 n_2^{-1} \in \omega_c$ for some $a \in B_c$, $n_1 \in N_1$ and $n_2 \in N_2$. Then $n_1 \in \omega_1$ and $n_2 \in \omega_2$.*

It is well known that $A_c N_c$ is closed in G_c and the mapping $(a, n) \to an$ $(a \in A_c, n \in N_c)$ of $A_c \times N_c$ into G_c is topological (see Iwasawa [5]). We define $\log n$ $(n \in N_c)$ as before and denote by t_α $(\alpha \in P)$ the Cartesian coordinates in the complex Euclidean space $\mathfrak{n}$ corresponding to the base $(X_\alpha)_{\alpha \in P}$. Then it would be enough to show that, under our assumptions, $t_\alpha(\log n_1)$ and $t_\alpha(\log n_2)$ remain bounded for every $\alpha \in P$. Put $\mathfrak{n}_\alpha = \sum_{0 < \beta < \alpha} CX_\beta$, and let π_α denote the projection of $\mathfrak{n}$ on $\mathfrak{n}_\alpha$ given by $\pi_\alpha X_\beta = X_\beta$ $(0 < \beta < \alpha)$ and $\pi X_\beta = 0$ $(\beta \geqq \alpha)$. Then from Lemma 2, there exists a polynomial function p_α on $\mathfrak{n}_\alpha \times \mathfrak{n}_\alpha \times \mathfrak{n}_\alpha$ such that

$$t_\alpha(\log(\exp X_1 \exp X_2 \exp X_3)) = t_\alpha(X_1 + X_2 + X_3) + p_\alpha(\pi_\alpha X_1, \pi_\alpha X_2, \pi_\alpha X_3)$$

for $X_1, X_2, X_3 \in \mathfrak{n}$. Now $n_2 a n_1 n_2^{-1} = a(a^{-1} n_2 a) n_1 n_2^{-1}$. Since ω_c is compact, it follows from what we have said above that if $a' n' \in \omega_c$ $(a' \in A_c, n' \in N_c)$, then $t_\alpha(\log n')$ remains bounded for every $\alpha \in P$. This shows that

$t_\alpha(\log(a^{-1}n_2an_1n^{-1}))$ must remain bounded for every $\alpha \in P$. Now suppose the assertion of the lemma is false. Then let β be the lowest root in P such that $|t_\beta(\log n_1)| + |t_\beta(\log n_2)|$ does not remain bounded when n_1, n_2 and a vary in such a way as to fulfill our assumptions. Put $X_i = \log n_i$ $(i = 1, 2)$. Then[4] $\log(a^{-1}n_2a) = \mathrm{Ad}(a^{-1})X_2$ and so it is clear that[5]

$$t_\beta(\log(a^{-1}n_2an_1n_2^{-1})) = t_\beta((\mathrm{Ad}(a^{-1}) - 1)X_2 + X_1) + p_\beta(\pi_\beta \mathrm{Ad}(a^{-1})X_2, \pi_\beta X_1, -\pi_\beta X_2).$$

Therefore

$$(\xi_\beta(a^{-1}) - 1)t_\beta(X_2) + t_\beta(X_1) = t_\beta(\log(a^{-1}n_2an_1n_2^{-1})) - p_\beta(\pi_\beta \mathrm{Ad}(a^{-1})X_2, \pi_\beta X_1, -\pi_\beta X_2).$$

Now it follows from the definition of β and the compactness of B_c that the right side remains bounded. Moreover, if $\beta \in P_1$, then $t_\beta(X_2) = 0$. On the other hand, if $\beta \in P_2$, then $t_\beta(X_1) = 0$ and $(\xi_\beta(a^{-1}) - 1)^{-1} = \xi_\beta(a)(1 - \xi_\beta(a))^{-1}$ remains bounded for $a \in B_c$. Therefore, in either case, we conclude from the above equation that $|t_\beta(X_1)| + |t_\beta(X_2)|$ remains bounded. As this contradicts the definition of β, the lemma is proved.

COROLLARY. *There exists a compact set ω^* in G_c^* with the following property. If $nan^{-1} \in \omega_c$ for some $n \in N_c$ and $a \in B_c$, then $n^* \in \omega^*$.*

From Lemma 1, $n = n_2n_1$ $(n_2 \in N_2, n_1 \in N_1)$. Hence $nan^{-1} = n_2an_1'n_2^{-1}$, where $n_1' = a^{-1}n_1an_1^{-1}$. Choose compact sets ω_1, ω_2 corresponding to Lemma 4. Then $n_2 \in \omega_2$. Moreover, since $N_1 \subset \Xi_c$, it follows that $n^* = n_2^* \in \omega_2^*$. Hence we can take $\omega^* = \omega_2^*$.

Now we come to the proof of Lemma 3. Let U be the real analytic subgroup of G_c corresponding to the compact real form $\mathfrak{u} = \mathfrak{k}_0 + (-1)^{\frac{1}{2}}\mathfrak{p}_0$ of $\mathfrak{g}$. Then U is compact and it is well known (see Iwasawa [5]) that $G = UA_cN_c = UN_cA_c$. This implies that $G_c = UN_2N_1A_c$. Moreover $\Xi_c \supset N_1A_c$. Now suppose $xax^{-1} \in \omega_c$ $(x \in G_c, a \in B_c)$. Then if $x = un_2n_1a'$ $(u \in U, n_2 \in N_2, n_1 \in N_1, a' \in A_c)$ and $n_1' = a^{-1}n_1an_1^{-1}$, we have

$$xax^{-1} = u(n_2an_1'n_2^{-1})u^{-1} \in \omega_c.$$

Therefore $n_2an_1'n_2^{-1} \in U\omega_cU$. Since $U\omega_cU$ is also compact, we can select sets ω_1, ω_2 in accordance with Lemma 4, corresponding to $U\omega_cU$. Then $n_2 \in \omega_2$ and $x \in U\omega_2N_1A_c \subset U\omega_2\Xi_c$. Hence $x^* \in \Omega_c^*$, where $\Omega_c^* = (U\omega_2)^*$. This completes the proof of Lemma 3.

---

[4] As usual $x \to \mathrm{Ad}(x)$ $(x \in G)$ denotes the adjoint representation.

[5] Here 1 stands for the identity mapping of $\mathfrak{g}$.

We now return to Theorem 1. Let Z be the center of G. Since $Z \subset \Xi$, it is clear that, for the proof of this theorem, we may replace G by any other connected group locally isomorphic to it. Let us therefore assume that G is the real analytic subgroup of G_c corresponding to $\mathfrak{g}_0$. Also, it will be convenient to suppose that G_c is simply connected. Let η be the conjugation of $\mathfrak{g}$ with respect to $\mathfrak{g}_0$. Then η can be "extended" to a (real) automorphism of G_c which we again denote by η. Since G is the connected component of the subgroup consisting of those points of G_c which are left fixed by η, G is closed in G_c. Also $A = A_c \cap G$ (see [4(c), § 2]) and $\Xi = G \cap \Xi_c$. Therefore $G^* = G/\Xi$ may be regarded as a subset of G_c^*. It is clear that Theorem 1 would follow immediately from Lemma 3 if we can show that G^* is closed in G_c^* and the inclusion mapping of G^* into G_c^* is topological. An elementary argument shows that this mapping is certainly continuous. Hence it is sufficient to prove the following result.

LEMMA 5. *Let $\{x_r^*\}_{r\geqq 1}$ be a sequence in G^* which converges in G_c^* to some point x^*. Then $x^* \in G^*$ and x_r^* converges to x^* in G^*.*

Define the structure of a Hilbert space on $\mathfrak{g}$ by means of the positive-definite Hermitian form $\| X \|^2 = -B(X, \bar{\theta}(X))$ $(X \in \mathfrak{g})$ as in [4(h), § 5] For any linear transformation T on $\mathfrak{g}$, put $\| T \|^2 = \mathrm{sp}(T^*T)$, where T^* is the adjoint of T. Then $\| X \| = \| \mathrm{ad}\, X \|$ $(X \in \mathfrak{g})$. We write $\| x \| = \| \mathrm{Ad}(x) \|$ $(x \in G_c)$ and call a subset ω' of G_c bounded if $\| x \|$ remains bounded for $x \in \omega'$. Since the center of G_c is finite, it is clear that ω' is bounded if and only if its closure in G_c is compact. Select points $x_r \in G$ and $x \in G_c$ lying in the cosets x_r^* and x^*, respectively. Then obviously $x_r a_0 x_r^{-1} \to x a_0 x^{-1}$ in G_c, and therefore $\| x_r a_0 x_r^{-1} \|$ remains bounded. But as we shall show below (Lemma 6) this implies that x_r^* are all contained in a compact subset of G^*, and from this, the assertion of Lemma 5 follows immediately. Thus it remains to prove the following lemma.

LEMMA 6. *Let ω be a compact set in G. Then there exists a compact subset Ω^* of G^* satisfying the condition that if $x a_0 x^{-1} \in \omega$ $(x \in G)$, then $x^* \in \Omega^*$.*

Let $\mathfrak{z}_0$ be the centralizer of a_0 in $\mathfrak{g}_0$. Then it follows from Lemma 7 of [4(c)] that $\theta(\mathfrak{z}_0) = \mathfrak{z}_0$, and therefore (see [4(h), Lemma 10]) $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$. Moreover $\mathfrak{h}_0 \subset \mathfrak{z}_0$, and therefore the ranks of $\mathfrak{g}_0$ and $\mathfrak{z}_0$ are the same. *Now it is convenient to drop our earlier notation and redefine $\mathfrak{h}_{\mathfrak{p}_0}$ and $\mathfrak{h}_0$ as follows.* Let $\mathfrak{h}_{\mathfrak{p}_0}$ be a maximal abelian subspace of $\mathfrak{z}_{\mathfrak{p}_0} = \mathfrak{z}_0 \cap \mathfrak{p}_0$. We extend it to a Cartan subalgebra $\mathfrak{h}_0$ of $\mathfrak{z}_0$. Then $\mathfrak{h}_0 = \mathfrak{h}_{\mathfrak{p}_0} + \mathfrak{h}_{\mathfrak{k}_0}$, where

$\mathfrak{h}_{\mathfrak{k}_0} = \mathfrak{h}_0 \cap \mathfrak{k}_0$, and since the ranks of $\mathfrak{g}_0$ and $\mathfrak{z}_0$ are equal and $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$, $\mathfrak{h}_0$ is also a Cartan subalgebra of $\mathfrak{g}_0$. We now introduce the notation[6] of [4(h), § 5] corresponding to the *new* $\mathfrak{h}_0$. In particular, A is now the Cartan subgroup of G corresponding to $\mathfrak{h}_0$ and $A_{\mathfrak{p}} = \exp \mathfrak{h}_{\mathfrak{p}_0}$. Since $\mathfrak{h}_0$ is contained in the centralizer of a_0, it is obvious that $a_0 \in A$. Let $a_0 = a_1 a_2$, where $a_1 \in A \cap K$ and $a_2 \in A_{\mathfrak{p}}$ (see [4(e), Lemma 7]). Clearly $\mathfrak{m}_{\mathfrak{p}_0}$ and $\mathfrak{n}_0$ are invariant under $\mathrm{Ad}(a_0)$. Moreover, since $\mathfrak{h}_{\mathfrak{p}_0}$ is maximal abelian in $\mathfrak{z}_{\mathfrak{p}_0}$, $\mathfrak{z}_{\mathfrak{p}_0} \cap \mathfrak{m}_{\mathfrak{p}_0} = \{0\}$. Therefore $\mathrm{Ad}(a_0)$ can never take the eigenvalue 1 in $\mathfrak{m}_{\mathfrak{p}_0}$. Put $\mathfrak{n}_0' = \mathfrak{z}_0 \cap \mathfrak{n}_0$ and let $\mathfrak{n}_0''$ be the orthogonal complement of $\mathfrak{n}_0'$ in $\mathfrak{n}_0$. Since $\mathrm{Ad}(a_1)$ is unitary and $\mathrm{Ad}(a_2)$ is self-adjoint and they commute, it follows that both $\mathfrak{n}_0'$ and $\mathfrak{n}_0''$ are invariant under $\mathrm{Ad}(a_0)$ and no eigenvalue of $\mathrm{Ad}(a_0)$ in $\mathfrak{n}_0''$ can be 1. The same argument shows that $\mathfrak{z}_{\mathfrak{p}_0}$ and $\mathfrak{m}_{\mathfrak{p}_0}$ are mutually orthogonal.

Now let $\mathfrak{z}$, $\mathfrak{m}_{\mathfrak{p}}$, $\mathfrak{h}$, $\mathfrak{n}'$, $\mathfrak{n}''$, $\mathfrak{n}$, $\mathfrak{g}_\lambda$ $(\lambda \in \mathfrak{F})$ denote the complexifications of $\mathfrak{z}_0$, $\mathfrak{m}_{\mathfrak{p}_0}$, $\mathfrak{h}_0$, $\mathfrak{n}_0'$, $\mathfrak{n}_0''$, $\mathfrak{n}_0$, $\mathfrak{g}_{0\lambda}$, respectively, in $\mathfrak{g}$ and similarly for the others. Since every element in $\mathrm{ad}(\mathfrak{h}_{\mathfrak{p}_0})$ is self-adjoint, both $\mathfrak{n}'$, $\mathfrak{n}''$ are invariant under $\mathrm{ad}(\mathfrak{h}_{\mathfrak{p}})$. Put $\mathfrak{n}_\lambda' = \mathfrak{n}' \cap \mathfrak{g}_\lambda$, $\mathfrak{n}_\lambda'' = \mathfrak{n}'' \cap \mathfrak{g}_\lambda$ $(\lambda \in \mathfrak{F})$. Then $\mathfrak{n}_\lambda'$ and $\mathfrak{n}_\lambda''$ are mutually orthogonal and invariant under $\mathrm{Ad}(a_0)$, and $\mathfrak{n}' = \sum_{\lambda>0} \mathfrak{n}_\lambda'$, $\mathfrak{n}'' = \sum_{\lambda>0} \mathfrak{n}_\lambda''$, where both sums are orthogonal. Moreover, $\mathrm{Ad}(a_0)$ never takes the eigenvalue 1 on $\mathfrak{n}_\lambda''$, while its restriction on $\mathfrak{n}'$ is the identity. Choose a base for $\mathfrak{g}_\lambda$ $(\lambda > 0)$ consisting of eigen-vectors of $\mathrm{Ad}(a_0)$. Then every element of this base lies either in $\mathfrak{n}_\lambda'$ or in $\mathfrak{n}_\lambda''$. Moreover, all these bases, put together for all $\lambda > 0$, form a base $(X_1, \cdots, X_q)$ for $\mathfrak{n}$. We number the elements X_i in such a way that if $X_i \in \mathfrak{g}_\lambda$, $X_j \in \mathfrak{g}_\mu$ and $0 < \lambda < \mu$, then $i < j$. Then it is obvious that $[X_i, X_j] \in \sum_{k>j} CX_k$ $(1 \leqq i < j \leqq q)$.

Let N, N', respectively, be the analytic subgroups of G corresponding to $\mathfrak{n}_0$, $\mathfrak{n}_0'$ and put $N'' = \exp \mathfrak{n}_0''$. Define M and $M_{\mathfrak{p}} = \exp \mathfrak{m}_{\mathfrak{p}_0}$ as in [4(h), § 5]. Then from Lemma 11 of [4(h)], $G = KM_{\mathfrak{p}}NA_{\mathfrak{p}}$, and it is obvious that $\Xi \supset N'A_{\mathfrak{p}}$. Moreover, it follows from Lemma 1 that $N = N''N'$. Finally, since G is imbedded in the complex group G_c, the center of G is finite, and therefore K is compact. Therefore, we may assume without loss of generality that $\omega = K\omega K$. Now suppose $x = kmna$ $(k \in K, m \in M_{\mathfrak{p}}, n \in N, a \in A_{\mathfrak{p}})$ and $xa_0x^{-1} \in \omega$. Then $(mna)a_0(mna)^{-1} \in \omega$, and therefore

$$a_0^{-1}ya_0y^{-1} = a_0^{-1}mna_0n^{-1}m^{-1} \in a_0^{-1}\omega,$$

[6] Unless it is explicitly stated otherwise, the various symbols $\mathfrak{m}_0$, $\mathfrak{m}_{\mathfrak{p}_0}$, $\mathfrak{n}_0$, $\mathfrak{g}_{0\lambda}$ $(\lambda \in \mathfrak{F})$ etc. are always meant to have the same meaning as in [4(h), § 5] corresponding to the *new* $\mathfrak{h}_0$.

where $y = mna$. On the other hand,

$$a_0^{-1}mna_0n^{-1}m^{-1} = (a_0^{-1}ma_0)m^{-1}m(a_0^{-1}na_0n^{-1})m^{-1}$$

and $(a_0^{-1}ma_0)m^{-1} \in M_{\mathfrak{p}}M_{\mathfrak{p}} \subset M \subset KM_{\mathfrak{p}}$ while $m(a_0^{-1}na_0n^{-1})m^{-1} \in mNm^{-1} = N$. Therefore, since $a_0^{-1}\omega$ is compact, it follows from Lemma 11 of [4(h)] that both $\| a_0^{-1}ma_0m^{-1} \|$ and $\| m(a_0^{-1}na_0n^{-1})m^{-1} \|$ must remain bounded (as x varies in G subject to the condition that $xa_0x^{-1} \in \omega$). However, as we shall see in Lemma 7, the boundedness of $\| a_0^{-1}ma_0m^{-1} \|$ implies that m remains within a compact subset of $M_{\mathfrak{p}}$. Since $\| m^{-1}zm \| \leqq \| m^{-1} \| \| z \| \| m \|$ for any $z \in G$, it follows that $\| a_0^{-1}na_0n^{-1} \|$ also remains bounded. Now let $n = n_2n_1$ ($n_1 \in N'$, $n_2 \in N''$). Then $a_0^{-1}na_0n^{-1} = a_0^{-1}n_2a_0n_2^{-1}$. But as we shall prove in Lemma 9, the boundedness of $\| a_0^{-1}n_2a_0n_2^{-1} \|$ implies the boundedness of $\| n_2 \|$. Then if $x_1 = kmn_2$, we have $x^* = x_1^*$ and $\| x_1 \| = \| mn_2 \| \leqq \| m \| \| n_2 \|$. This shows that x_1 stays within a bounded subset of G, and therefore $x^* = x_1^*$ within a compact subset of G^*. Hence our assertion is now proved.

We have still to prove the two results which were used above.

LEMMA 7. *Suppose m varies in $M_{\mathfrak{p}}$ in such a way that $\| ma_0m^{-1} \|$ remains bounded. Then $\| m \|$ also remains bounded.*

Define a_1, a_2 as above. Then $a_0 = a_1a_2$ and a_2 commutes with every element in $M_{\mathfrak{p}}$ since $[\mathfrak{h}_{\mathfrak{p}_0}, \mathfrak{m}_{\mathfrak{p}_0}] = \{0\}$. Therefore $ma_0m^{-1} = (ma_1m^{-1})a_2$, and so $\| ma_1m^{-1} \|$ remains bounded. Moreover, the exponential mapping being one-one and regular on $\mathfrak{p}_0$, we may denote by log its inverse on $\exp \mathfrak{p}_0$. Then it would be sufficient to show that $\| \log m \|$ remains bounded. For this we need the following lemma.

LEMMA 8. *Let k be an element in K. Then if $n = \dim_C \mathfrak{g}$,*

$$\| pkp^{-1} \| \geqq n^{\frac{1}{2}} \cosh(n^{-\frac{1}{2}} \| \log p - \mathrm{Ad}(k)(\log p) \|)$$

for for $p \in \exp \mathfrak{p}_0$.

Assuming this for a moment, Lemma 7 can now be proved as follows. We have seen that $\mathrm{Ad}(a_0)$ never takes the eigenvalue 1 in $\mathfrak{m}_{\mathfrak{p}_0}$ and $\mathrm{Ad}(a_0) = \mathrm{Ad}(a_1)$ on $\mathfrak{m}_{\mathfrak{p}_0}$. Hence we can find a positive number c such that $\| X - \mathrm{Ad}(a_1)X \| \geqq c \| X \|$ for all $X \in \mathfrak{m}_{\mathfrak{p}_0}$. Therefore, from Lemma 8,

$$\| ma_1m^{-1} \| \geqq n^{\frac{1}{2}} \cosh(n^{-\frac{1}{2}}c \| \log m \|)$$

for all $m \in M_{\mathfrak{p}}$. But as we have seen above $\| ma_1m^{-1} \|$ remains bounded under the assumptions of Lemma 7, and so the same holds for $\| \log m \|$ and $\| m \|$.

Now in order to prove Lemma 8, we proceed as follows. Let E be the

space of all endomorphisms of $\mathfrak{g}$. Put $\langle S, T\rangle = \mathrm{sp}(S^*T)$ $(S, T \in E)$, where S^* is the adjoint of S. This scalar product defines the structure of a Hilbert space on E. Let d_X $(X \in \mathfrak{g})$ denote the linear mapping of E given by $d_X T = [\mathrm{ad}\, X, T]$, where $[S, T] = ST - TS$ $(S, T \in E)$. If $X \in \mathfrak{p}_0$, $\mathrm{ad}\, X$ is self-adjoint, and therefore

$$\begin{aligned}\langle S, d_X T\rangle &= \mathrm{sp}(S^*[\mathrm{ad}\, X, T]) = -\mathrm{sp}([\mathrm{ad}\, X, S^*]T)\\ &= \mathrm{sp}((d_X S)^* T) = \langle d_X S, T\rangle.\end{aligned}$$

This proves that d_X is also self-adjoint. Moreover, if $p = \exp X \in \exp \mathfrak{p}_0$, it is obvious (by considering E as a Lie algebra under the bracket operation $[S, T]$) that $\exp d_X$ is the mapping σ_p: $T \to \mathrm{Ad}(p) T \,\mathrm{Ad}(p^{-1})$ $(T \in E)$ of E. Clearly σ_p is also self-adjoint. Hence we can choose an orthonormal base $(T_1, \cdots, T_r)$ of E consisting of eigen-vectors of d_X and σ_p. Let λ_i be the eigenvalue of d_X corresponding to T_i $(1 \leqq i \leqq r)$. Then if $T = \sum_{1\leqq i\leqq r} c_i T_i$ $(c_i \in C)$, it is clear that $\sigma_p T = \sum_i c_i e^{\lambda_i} T_i$, and therefore $\| \sigma_p T \|^2 = \sum_i | c_i |^2 e^{2\lambda_i}$. Now put $T = \mathrm{Ad}(k)$, where k is some fixed element in K. Then this equation becomes

$$\| pkp^{-1} \|^2 = \sum_{1\leqq i\leqq r} | c_i |^2 e^{2\lambda_i}.$$

On the other hand, since $\| Y \| = \| \theta(Y) \|$ $(Y \in \mathfrak{g})$, θ is a unitary transformation of $\mathfrak{g}$, and therefore $\| \theta S \theta^{-1} \| = \| S \|$ for any $S \in E$. Moreover, since $\theta(X) = -X$, it follows that $\theta(\mathrm{Ad}(pkp^{-1}))\theta^{-1} = \mathrm{Ad}(p^{-1}kp)$. Therefore

$$\begin{aligned}2 \| pkp^{-1} \|^2 &= \| pkp^{-1} \|^2 + \| p^{-1}kp \|^2 = \| \sigma_p T \|^2 + \| \sigma_{p^{-1}} T \|^2\\ &= 2 \sum_{1\leqq i\leqq r} | c_i |^2 \cosh 2\lambda_i.\end{aligned}$$

But $\cosh 2t = 1 + 2 \sinh^2 t$ and $s(t) = \sinh t / t = \sum_{q\geqq 0} t^{2q}/(2q+1)!$ is an increasing function of t for $t \geqq 0$. Therefore

$$\| pkp^{-1} \|^2 = \sum_{1\leqq i\leqq r} | c_i |^2 + 2 \sum_{1\leqq i\leqq r} | c_i \lambda_i |^2 s(\lambda_i)^2.$$

Moreover, $\sum_i | c_i |^2 = \| k \|^2 = n$ since $\mathrm{Ad}(k)$ is unitary. Now choose an index j $(1 \leqq j \leqq r)$ such that $| c_j \lambda_j | = \max_{1\leqq i\leqq r} | c_i \lambda_i |$. Since $| c_j | \leqq \| k \| = n^{\frac{1}{2}}$, it follows that $s(n^{-\frac{1}{2}} | c_j \lambda_j |) \leqq s(| \lambda_j |)$, and therefore

$$\begin{aligned}\| pkp^{-1} \|^2 &\geqq n + 2 | c_j \lambda_j |^2 s(\lambda_j)^2 \geqq n + 2 | c_j \lambda_j |^2 \{ s(n^{-\frac{1}{2}} | c_j \lambda_j |) \}^2\\ &= n \cosh(2n^{-\frac{1}{2}} | c_j \lambda_j |).\end{aligned}$$

On the other hand, $\| d_X T \|^2 = \sum_{1 \leqq i \leqq r} | c_i \lambda_i |^2 \leqq r \, | c_j \lambda_j |^2$ and $r = \dim E = n^2$. Therefore $| c_j \lambda_j | \geqq n^{-1} \| d_X T \|$ and

$$\| pkp^{-1} \| \geqq n^{\frac{1}{2}} \cosh (n^{-\frac{3}{2}} \| d_X T \|)$$

since $\cosh t$ is an increasing function of t for $t \geqq 0$ and $\cosh 2t \geqq \cosh^2 t$. But $T = \mathrm{Ad}(k)$ is unitary, and therefore

$$\begin{aligned} \| d_X T \| = \| (d_X T) T^{-1} \| &= \| (\mathrm{ad}\, X) - T(\mathrm{ad}\, X) T^{-1} \| \\ &= \| \mathrm{ad}(X - \mathrm{Ad}(k)X) \| = \| X - \mathrm{Ad}(k) X \|. \end{aligned}$$

This proves that

$$\| pkp^{-1} \| \geqq n^{\frac{1}{2}} \cosh (n^{-\frac{3}{2}} \| X - \mathrm{Ad}(k) X \|)$$

which is equivalent to the statement of Lemma 8.

The second result which was required during the proof of Lemma 6, may be stated as follows.

LEMMA 9. *Suppose n varies in N'' in such a way that $\| a_0^{-1} n a_0 n^{-1} \|$ remains bounded. Then $\| n \|$ itself remains bounded.*

Consider the base $(X_1, \cdots, X_q)$ of $\mathfrak{n}$ introduced during the proof of Lemma 6 and let $(t_1, \cdots, t_q)$ denote the complex Cartesian coordinates in $\mathfrak{n}$ corresponding to this base. For any j $(1 \leqq j \leqq q)$, define the projection π_j as in Lemma 2, and put $\pi_0 = 0$ and $\mathfrak{n}_j = \pi_j \mathfrak{n}$ $(0 \leqq j \leqq q)$. Then from Lemma 2, there exist polynomial functions p_j on $\mathfrak{n}_{j-1} \times \mathfrak{n}_{j-1}$ such that

$$t_j(\log(\exp Y_1 \exp Y_2)) = t_j(Y_1 + Y_2) + p_j(\pi_{j-1} Y_1, \pi_{j-1} Y_2) \quad (1 \leqq j \leqq q)$$

for $Y_1, Y_2 \in \mathfrak{n}$. Now put $X = \log n$. Then it would be enough to prove that $t_j(X)$ $(1 \leqq j \leqq q)$ all remain bounded. Suppose this is false. Then consider the least index j such that $| t_j(X) |$ does not stay bounded. Put

$$Z = \log(a_0^{-1} n a_0 n^{-1}) = \log(\exp(\mathrm{Ad}(a_0^{-1}) X) \exp(-X)).$$

Then

$$t_j(Z) = t_j(\mathrm{Ad}(a_0^{-1}) X) - t_j(X) + p_j(\pi_{j-1} \mathrm{Ad}(a_0^{-1}) X, -\pi_{j-1} X).$$

But since X_i is an eigenvector of $\mathrm{Ad}(a_0)$, $\mathrm{Ad}(a_0) X_i = c_i X_i$ $(1 \leqq i \leqq q)$, where c_i are nonzero complex numbers. Therefore $t_i(\mathrm{Ad}(a_0^{-1}) X) = c_i^{-1} t_i(X)$ and

$$(c_j^{-1} - 1) t_j(X) = t_j(Z) - p_j(\pi_{j-1} \mathrm{Ad}(a_0^{-1}) X, -\pi_{j-1} X).$$

In view of the hypothesis of the lemma and our choice of j, the right side remains bounded as n varies. Moreover, $c_j \neq 1$ if $X_j \in \mathfrak{n}''$, and $t_j(X) = 0$ if $X_j \in \mathfrak{n}'$. Therefore, it follows from the above equation that $t_j(X)$ remains

3

bounded in either case. As this contradicts the definition of j, the lemma is proved.

The proof of Theorem 1 is now quite complete.

3. The sets V and V_G. In order to prove our next result, we need a simple lemma. Let W be a vector space over C of finite dimension. We shall call an endomorphism X of W unipotent if $X-1$ is nilpotent. (Here 1 stands for the identity mapping of W.)

LEMMA 10. *Let $\mathfrak{N}$ and $\mathcal{E}$, respectively, be the sets of all nilpotent and unipotent endomorphisms of W. Then $X \to \exp X$ $(X \in \mathfrak{N})$ is a one-one mapping of $\mathfrak{N}$ onto $\mathcal{E}$.*

Since $\exp X - 1 = \sum_{k \geqq 1} X^k/k!$, it is obvious that $\exp X \in \mathcal{E}$ for $X \in \mathfrak{N}$. For any $Y \in \mathcal{E}$, define $\log Y = \sum_{k \geqq 1} (-1)^{k-1}(Y-1)^k/k$. Since Y is unipotent, this series is actually finite, and it is clear that $\log Y \in \mathfrak{N}$. Our assertion now follows from the well-known identities (see Birkhoff [1]) $X = \log(\exp X)$ $(X \in \mathfrak{N})$ and $Y = \exp(\log Y)$ $(Y \in \mathcal{E})$.

Now G being as in Theorem 1, we shall prove the following result.

LEMMA 11. *Let V be the open set in the real Euclidean space $\mathfrak{g}_0$ defined as follows. An element X of $\mathfrak{g}_0$ lies in V if and only if the absolute value of every eigenvalue of $\operatorname{ad} X$ is less than[7] π. Then the exponential mapping of $\mathfrak{g}_0$ into G is regular and univalent on V.*

If $X \in V$, it is clear that $\operatorname{ad} X$ can never have an eigenvalue of the form $2\pi(-1)^{\frac{1}{2}}n$ where n is a nonzero integer. Therefore

$$(1-\exp(-\operatorname{ad} X))/\operatorname{ad} X = \sum_{m \geqq 0} (-1)^m (\operatorname{ad} X)^m/(m+1)!$$

is a nonsingular transformation of $\mathfrak{g}_0$. This shows (see Chevalley [2(a), p. 157]) that the exponential mapping is regular at X. Now suppose $\exp X_1 = \exp X_2$ $(X_1, X_2 \in V)$. Put $\sigma = (1-\exp(-\operatorname{ad} X_1))/\operatorname{ad} X_1$. Then $\operatorname{Ad}(x) - 1 = \exp(\operatorname{ad} X_1) - 1 = \operatorname{Ad}(x)\sigma \operatorname{ad} X_1$, where $x = \exp X_1 = \exp X_2$. Since $\operatorname{Ad}(x)$ and σ are both nonsingular, it follows that $\operatorname{Ad}(x)Y = Y$ for some $Y \in \mathfrak{g}$ if and only if $(\operatorname{ad} X_1)Y = 0$. Let $\mathfrak{c}_0$ denote the centralizer of x in $\mathfrak{g}_0$. Then $\mathfrak{c}_0$ is also the centralizer of X_1 in $\mathfrak{g}_0$. But obviously $\operatorname{Ad}(x)X_2 = X_2$, and therefore X_1, X_2 commute. Hence $\exp(X_1 - X_2) = \exp X_1 \exp(-X_2) = 1$. Let λ_{ji} $(1 \leqq j \leqq r_i)$ denote all the distinct eigenvalues of $\operatorname{ad} X_i$ $(i = 1, 2)$. Then every eigenvalue of $\operatorname{ad}(X_1 - X_2)$ must be

[7] Here π denotes, as usual, the smallest positive root of the equation $\sin t = 0$.

of the form $\lambda_{j1}-\lambda_{k2}$ for some j and k. Moreover it follows from the definition of V that $|\lambda_{j1}-\lambda_{k2}|<2\pi$. Hence $\exp(\lambda_{j1}-\lambda_{k2})\neq 1$ unless $\lambda_{j1}=\lambda_{k2}$. Therefore since $\exp\operatorname{ad}(X_1-X_2)=\operatorname{Ad}(\exp(X_1-X_2))=1$, zero is the only eigenvalue of $\operatorname{ad}(X_1-X_2)$. This implies that $\operatorname{ad}(X_1-X_2)$ is nilpotent, and so it follows from Lemma 10 that $\operatorname{ad}(X_1-X_2)=0$. But $\mathfrak{g}$ being semisimple, we can now conclude that $X_1=X_2$, and therefore the exponential mapping is univalent on V.

Let V_G denote the image of V in G under the exponential mapping and let Z denote the center of G. Obviously V_G is open in G.

COROLLARY. *If $z\in Z$ then V_G does not intersect zV_G unless $z=1$.*

This follows by applying Lemma 11 to G/Z instead of G.

The following property of V is important for our applications.

LEMMA 12. *Let X_r $(r\geqq 1)$ be a sequence in V. Then if $\|\exp X_r\|$ remains bounded, the same holds for $\|X_r\|$.*

For the purpose of this lemma we can obviously replace G by any connected group locally isomorphic to it. Hence we may assume that $G\subset G_c$ (see § 2). We shall now use the notation of the proofs of Lemmas 3 and 4. Put $\mathfrak{g}_1=\bigcup_{u\in U}\operatorname{Ad}(u)(\mathfrak{h}+\mathfrak{n})$. Since $G=UA_cN_c$ and $\mathfrak{h}+\mathfrak{n}$ is invariant under $\operatorname{Ad}(A_cN_c)$, it is obvious that $\operatorname{Ad}(x)\mathfrak{g}_1=\mathfrak{g}_1$ for $x\in G_c$. Since every regular element of $\mathfrak{g}$ is conjugate to some element in $\mathfrak{h}$ under G_c (see Chevalley [2(b)]), $\mathfrak{g}_1$ contains the set of all regular elements in $\mathfrak{g}$. On the other hand, since U is compact it is clear that $\mathfrak{g}_1$ is closed in $\mathfrak{g}$. Therefore, since regular elements are dense in $\mathfrak{g}$, $\mathfrak{g}=\mathfrak{g}_1$. Hence we can choose $u_r\in U$ and $Y_r\in\mathfrak{h}+\mathfrak{n}$ such that $X_r=\operatorname{Ad}(u_r)Y_r$. Since $\operatorname{Ad}(u_r)$ is unitary, $\|X_r\|=\|Y_r\|$ and $\|\exp X_r\|=\|\exp Y_r\|$. Let $Y_r=H_r+Z_r$ $(H_r\in\mathfrak{h}, Z_r\in\mathfrak{n})$. One proves without difficulty that the eigenvalues of $\operatorname{ad}Y_r$ and $\operatorname{ad}H_r$ are the same. Therefore since $X_r\in V$, it follows that $|\alpha(H_r)|<\pi$ for every root $\alpha\in P$. This shows that $\|H_r\|$ remains bounded. Now let $F(t)$ denote the entire function on the complex plane given by the series

$$F(t)=\sum_{m\geqq 0}(-1)^m t^m/(m+1)!=(1-e^{-t})/t.$$

Let H_0 be a fixed element in $\mathfrak{h}$ and let t_α $(\alpha\in P)$ denote the complex Cartesian coordinates in $\mathfrak{n}$ corresponding to the base X_α $(\alpha\in P)$. Then if $H\in\mathfrak{h}$ and $Z\in\mathfrak{n}$, it is obvious that $\operatorname{Ad}(\exp(H+Z))H_0-H_0\in\mathfrak{n}$. For any $\beta\in P$, consider the function

$$f_\beta(H,Z)=t_\beta(\operatorname{Ad}(\exp(H+Z))H_0-H_0)+e^{\beta(H)}F(\beta(H))\beta(H_0)t_\beta(Z)$$

on $\mathfrak{h}+\mathfrak{n}$ $(H\in\mathfrak{h}, Z\in\mathfrak{n})$. Obviously, it is holomorphic. Moreover, if $\beta<\gamma$ $(\gamma\in P)$, it is easily seen that $f_\beta(H,Z+tX_\gamma)=f_\beta(H,Z)$ $(t\in C)$. Hence f_β depends only on H and $t_\alpha(Z)$ $(0<\alpha\leqq\beta)$. Let us now consider $\{(d/dt)f_\beta(H,Z+tX_\beta)\}_{t=0}$. We know (see Chevalley [2(a), p. 157]) that

$$\{(d/dt)\operatorname{Ad}(\exp(H+Z+tX_\beta))H_0\}_{t=0}=\operatorname{Ad}(\exp(H+Z))(\operatorname{ad}Y)H_0,$$

where

$$\begin{aligned}Y&=\{(1-\exp(-\operatorname{ad}(H+Z)))/\operatorname{ad}(H+Z)\}X_\beta\\&\equiv F(\beta(H))X_\beta \mod \sum_{\gamma>\beta}CX_\gamma.\end{aligned}$$

Therefore

$$\begin{aligned}\{(d/dt)f_\beta(H,Z+tX_\beta)\}_{t=0}=F(\beta(H))t_\beta(\operatorname{Ad}(\exp(H+Z))[X_\beta,H_0])\\+e^{\beta(H)}F(\beta(H))\beta(H_0).\end{aligned}$$

But $[X_\beta,H_0]=-\beta(H_0)X_\beta$ and $\operatorname{Ad}(\exp(H+Z))X_\beta\equiv e^{\beta(H)}X_\beta \mod \sum_{\gamma>\beta}CX_\gamma$. Hence, it follows that $\{(d/dt)f_\beta(H+Z+tX_\beta)\}_{t=0}=0$, and therefore f_β depends only on H and $t_\alpha(Z)$ $(0<\alpha<\beta)$.

Now suppose the assertion of the lemma is false. Then there exists a root $\beta\in P$ such that $t_\beta(Z_r)$ does not remain bounded. Select the least such root β. Then $\|H_r\|$ and $t_\alpha(Z_r)$ $(0<\alpha<\beta)$ all remain bounded and therefore $f_\beta(H_r,Z_r)$ also remains bounded as $r\to\infty$. On the other hand, by our hypothesis, $\|\exp Y_r\|$, and therefore, also, $\|\operatorname{Ad}(\exp(H_r+Z_r))\|$ stay bounded. Hence the same holds for

$$e^{\beta(H_r)}F(\beta(H_r))\beta(H_0)t_\beta(Z_r)=f_\beta(H_r,Z_r)-t_\beta(\operatorname{Ad}(\exp(H_r+Z_r))H_0-H_0).$$

On the other hand, $|\beta(H_r)|<\pi$, and so $e^{-\beta(H_r)}\{F(\beta(H_r))\}^{-1}$ also remains bounded. Therefore by choosing H_0 in such a way that $\beta(H_0)\neq 0$, we conclude that $t_\beta(Z_r)$ also remains bounded. As this contradicts the definition of β, the lemma follows.

Let us say that a sequence x_r $(r\geqq 1)$ in G tends to infinity, if for every compact set ω of G, we can select a positive integer r_0 such that $x_r\notin\omega$ for $r\geqq r_0$. Obviously if $x_r\to\infty$, the same holds for any subsequence of $\{x_r\}$.

COROLLARY. *Let z_r $(r\geqq 1)$ be a sequence in Z which tends to infinity. Then if $x_r\in z_rV_G$, x_r also tends to infinity.*

For otherwise, by selecting a subsequence, we can arrange that x_r converges to some $x\in G$. But $x_r=z_r\exp X_r$, where $X_r\in V$ and $\|x_r\|=\|\exp X_r\|$ remains bounded. Therefore by Lemma 12, $\|X_r\|$ also remains bounded

and so again by selecting a subsequence, we may suppose that X_r converges to some $X \in \mathfrak{g}_0$. Then $z_r = x_r \exp(-X_r) \to x \exp(-X)$, contradicting our hypothesis that $z_r \to \infty$.

Part II.

4. Proof of Theorem 2. Let A be a Cartan subgroup of G (see [4(c), §2]) and $\mathfrak{h}_0$ the Lie algebra of A. We assume that $\theta(\mathfrak{h}_0) = \mathfrak{h}_0$. Let $x \to x^*$ $(x \in G)$ denote the natural mapping of G on $G^* = G/A$ and put $h^{x^*} = xhx^{-1}$ $(x \in G, h \in A)$. We shall call a subset of G bounded if its closure is compact.

LEMMA 13. *Let ω be a bounded set in G and B the set of all $h \in A$ such that $h^{x^*} \in \omega$ for some $x^* \in G^*$. Then B is also bounded.*

Let h_r $(r \geqq 1)$ be a sequence of points in B. We have to show that some subsequence of $\{h_r\}$ is convergent. Choose $x_r \in G$ such that $h_r^{x_r^*} \in \omega$, and for any $y \in G$, define $\lambda(y)$ as follows. If $\lambda_1, \cdots, \lambda_s$ are all the distinct eigenvalues of $\mathrm{Ad}(y)$ and m_i is the multiplicity of λ_i, then

$$\lambda(y) = m_1 |\lambda_1|^2 + \cdots + m_s |\lambda_s|^2.$$

Since ω is bounded, we can find a positive number M such that $\lambda(y) \leqq M$ for all $y \in \omega$. Hence $\lambda(h_r) = \lambda(h_r^{x_r^*}) \leqq M$. But it is obvious that $\lambda(h) = \| h \|^2$ for $h \in A$ (in the notation of §2). Therefore $\| h_r \|^2 \leqq M$, and so by selecting a subsequence, we can arrange that $\mathrm{Ad}(h_r)$ is convergent. Choose $h_\infty \in A$ such that $\mathrm{Ad}(h_r) \to \mathrm{Ad}(h_\infty)$. Then $\mathrm{Ad}(h_r'') \to 1$ if $h_r'' = h_r h_\infty^{-1}$, and Z being the center of G, it is obvious that we can select $z_r \in Z$ such that $h_r' = z_r^{-1} h_r''$ converges to 1 in G. Since $h_r = z_r h_r' h_\infty$, it is enough to show that some subsequence of z_r is convergent or, what is equivalent, that z_r cannot tend to infinity. Let Ξ_∞ denote the centralizer of h_∞ in G and $\bar{x}_r$ the coset $x_r \Xi_\infty$ in G/Ξ_∞. Since $\mathrm{Ad}(h_r) \to \mathrm{Ad}(h_\infty)$ and $h_r^{x_r^*} \in \omega$, we can, by applying Theorem 1 to $\mathrm{Ad}(G) \cong G/Z$ at the point $\mathrm{Ad}(h_\infty)$, conclude that $\bar{x}_r$ are all contained in a compact subset of G/Ξ_∞. But $z_r (h_r')^{x_r^*} = (h_r h_\infty^{-1})^{x_r^*}$. Therefore, since $h_r^{x_r^*} \in \omega$, the right side remains within a compact subset of G. Moreover $h_r' \to 1$, and so we can assume without loss of generality that $h_r' \in V_G$ (in the notation of §3). Then $(h_r')^{x_r^*}$ is also in V_G, and hence it follows from the Corollary of Lemma 12 that z_r cannot tend to infinity. This proves the lemma.

From now on let us agree to use the notation of [4(h), §5]. For any $\alpha \in P$, let η_α denote the character of A given by $\mathrm{Ad}(h) X_\alpha = \eta_\alpha(h) X_\alpha$ $(h \in A)$. Put

$$\Delta'(h) = \prod_{\alpha \in P} (1 - \eta_\alpha(h^{-1})) \qquad (h \in A).$$

Let A' be the set of those points $h \in A$ where $\Delta'(h) \neq 0$. Then A' is exactly the set of regular elements in A (see [4(c), § 2]). Let dx^* denote the invariant measure on $G^* = G/A$.

LEMMA 14. Put[1]

$$F_f(h) = \Delta'(h) \int_{G^*} f(h^{x^*}) dx^* \qquad (h \in A', f \in C_c^\infty(G)).$$

Then the above integral is convergent and F_f is a function of class C^∞ on A'.

Fix $f \in C_c^\infty(G)$ and $h_0 \in A'$, and select a compact set ω in G such that f is zero outside ω. Then if Ξ is the centralizer of h_0 in G, it follows from the Corollary of Lemma 3 of [4(c)] that Ξ/A is finite. Hence by Theorem 1, we can select an open neighborhood B of h_0 in A' and a compact set Ω^* in G^* with the following property. If $xhx^{-1} \in \omega$ for some $h \in B$ and $x \in G$, then $x^* \in \Omega^*$. Therefore it is clear that

$$\int_{G^*} f(h^{x^*}) dx^* = \int_{\Omega^*} f(h^{x^*}) dx^* \qquad (h \in B),$$

and from this our lemma follows immediately.

Let $\mathfrak{B}$ be the universal enveloping algebra of $\mathfrak{g}$ and $\mathfrak{H}$ the subalgebra of $\mathfrak{B}$ generated by $(1, \mathfrak{h})$. Then we can regard the elements of $\mathfrak{B}$ and $\mathfrak{H}$ as left-invariant differential operators on G and A, respectively (see [4(c), § 4]). $S(\mathfrak{h})$ being the symmetric algebra over $\mathfrak{h}$, there exists a unique isomorphism of $S(\mathfrak{h})$ onto $\mathfrak{H}$ which preserves 1 and also every element in $\mathfrak{h}$. For any $q \in S(\mathfrak{h})$, we denote by $\partial(q)$ the image of q under this isomorphism. Then $\partial(q)$ is a differential operator on A.

Let A_1 be an open subset of A. We regard it as an open submanifold of A and consider the space $\mathscr{C}_0(A_1)$ of all complex-valued functions g on A_1 of class C^∞ satisfying the following two conditions.

(1) g vanishes (on A_1) outside some bounded subset of A_1.

(2) For every[1] $v \in \mathfrak{H}$,

$$\tau_v(g) = \sup_{h \in A_1} |g(h; v)| < \infty.$$

Define a topology in $\mathscr{C}_0(A_1)$ by means of the collection of seminorms τ_v ($v \in \mathfrak{H}$). Then $\mathscr{C}_0(A_1)$ is a locally convex space and the same holds for $C_c^\infty(G)$ under its usual topology (see Schwartz [6, p. 67]). Our main object now is to prove the following theorem.

THEOREM 2. *Let*

$$F_f(h) = \Delta'(h) \int_{G^*} f(h^{x^*}) dx^* \qquad (h \in A', f \in C_c^\infty(G)).$$

Then $F_f \in \mathcal{B}_0(A')$, *and* $f \to F_f$ *is a continuous mapping of* $C_c^\infty(G)$ *into* $\mathcal{B}_0(A')$. *Moreover, for any bounded open subset* ω *of* G, *we can select a bounded subset* B *of* A' *such that* F_f *is zero outside* B *for every*[1] $f \in C_c^\infty(\omega)$.

We begin by first proving the following weaker result.

LEMMA 15. *There exists an open neighborhood* ${}_0A$ *of* 1 *in* A *with the following property. Put* ${}_0A' = {}_0A \cap A'$ *and let* ${}_0F_f$ *denote the restriction of* F_f *on* ${}_0A'$ $(f \in C_c^\infty(G))$. *Then* ${}_0F_f \in \mathcal{B}_0({}_0A')$, *and* $f \to {}_0F_f$ *is a continuous mapping of* $C_c^\infty(G)$ *into* $\mathcal{B}_0({}_0A')$.

Let l be the rank of $\mathfrak{g}$ and n the complex dimension of $\mathfrak{g}$. Then if λ is an indeterminate and I the identity mapping of $\mathfrak{g}$,

$$\det(\lambda I - \operatorname{ad} X) = \lambda^n + \sum_{l \leqq r < n} (-1)^r p_r(X) \lambda^r \qquad (X \in \mathfrak{g}),$$

where[8] $p_r \in I(\mathfrak{g})$. Then if ϵ is a sufficiently small positive number, the inequalities $|p_r(X)| \leqq \epsilon$ $(l \leqq r < n)$ imply that every eigenvalue of $\operatorname{ad} X$ is less that $\pi/2$ in absolute value. Choose a function $\phi(t)$ of class C^∞ of $(n-l)$ real variables t_r $(l \leqq r < n)$ such that $\phi(t) = 0$ unless $\max_r |t_r| \leqq \epsilon$ and $\phi(t) = 1$ if $\max_r |t_r| \leqq \epsilon/2$. Let $\Phi(X)$ denote the function on $\mathfrak{g}_0$ obtained from ϕ under the substitution $t_r = p_r(X)$ $(X \in \mathfrak{g}_0)$. Define V as in §3 and let V_0 be the set of those $X \in V$ where $\max_r |p_r(X)| < \epsilon/3$. Then obviously, V_0 is an open neighborhood of zero in V and $\operatorname{Ad}(x) V_0 = V_0$ $(x \in G)$. For a given $f \in C_c^\infty(G)$, consider the function $\bar{f}$ on $\mathfrak{g}_0$ defined by $\bar{f}(X) = f(\exp X)\Phi(X)$ $(X \in \mathfrak{g}_0)$. It is obvious that the carrier of $\bar{f}$ is contained in V and $\bar{f}(X) = f(\exp X)$ for $(X \in V_0)$. Now define $x^*H = \operatorname{Ad}(x)H$ $(x \in G, H \in \mathfrak{h})$ and $\pi = \prod_{\alpha \in P} \alpha$. Let $\mathfrak{h}_0'$ be the set of those points $H \in \mathfrak{h}_0$ where $\pi(H) \neq 0$. The function $(1 - e^{-z})/z$ of the complex variable z, is holomorphic at $z = 0$ and takes the value 1 there. Therefore, since $\eta_\alpha(\exp H) = e^{\alpha(H)}$ $(H \in \mathfrak{h}_0)$, it is clear that we can select an open neighborhood $\mathfrak{h}_2$ of zero in $\mathfrak{h}_0 \cap V_0$ and an analytic function ζ on $\mathfrak{h}_2$ such that

$$\Delta'(\exp H) = \zeta(H)\pi(H) \qquad (H \in \mathfrak{h}_2).$$

Choose another open neighborhood $\mathfrak{h}_1$ of zero in $\mathfrak{h}_0$ such that the closure of $\mathfrak{h}_1$ is compact and contained in $\mathfrak{h}_2$. Obviously, $\zeta(o) = 1$ and ζ is never

---

[8] We are using here the notation of [4(g)].

zero on $\mathfrak{h}_2$. Put $\mathfrak{h}_1' = \mathfrak{h}_1 \cap \mathfrak{h}_0'$ and ${}_0A = \exp \mathfrak{h}_1$. Then ${}_0A$ is an open neighborhood of 1 in A and $\exp H \in {}_0A' = {}_0A \cap A'$ if $H \in \mathfrak{h}_1'$. For any $g \in C_c^\infty(\mathfrak{g}_0)$, put

$$\phi_g(H) = \pi(H) \int_{G^*} g(x^*H)\, dx^* \qquad (H \in \mathfrak{h}_1').$$

It follows from Theorem 3 of [4(h)] that the above integral is convergent and[8] $\phi_g \in \mathcal{C}(\mathfrak{h}_1')$. Moreover, it is obvious that $F_f(\exp H) = \zeta(H)\phi_{\bar{f}}(H)$ $(H \in \mathfrak{h}_1')$. But it follows from the definition of $\mathfrak{h}_1$, that[9] $\partial(q)\zeta$ remains bounded on $\mathfrak{h}_1$ for every $q \in S(\mathfrak{h})$. Therefore $\phi \to \zeta\phi$ $(\phi \in \mathcal{C}(\mathfrak{h}_1'))$ is a continuous mapping of $\mathcal{C}(\mathfrak{h}_1')$ into itself. In view of Theorem 3 of [4(h)], this proves that $g \to \zeta\phi_g$ $(g \in C_c^\infty(\mathfrak{g}_0))$ is a continuous mapping of $C_c^\infty(\mathfrak{g}_0)$ into $\mathcal{C}(\mathfrak{h}_1')$. On the other hand, ${}_0A' = \exp \mathfrak{h}_1'$ and, since the exponential mapping is one-one and regular on $\mathfrak{h}_2$ and the closure of $\mathfrak{h}_1$ is compact, it is clear that a function ψ on ${}_0A'$ lies in $\mathcal{C}_0({}_0A')$ if and only if the function $\psi'(H) = \psi(\exp H)$ $(H \in \mathfrak{h}_1')$ lies in $\mathcal{C}(\mathfrak{h}_1')$. Moreover, it is obvious that $\psi \to \psi'$ is a topological mapping of $\mathcal{C}_0({}_0A')$ onto $\mathcal{C}(\mathfrak{h}_1')$. Put $F_f'(H) = F_f(\exp H)$ $(f \in C_c^\infty(G), H \in \mathfrak{h}_1')$. Then it would be enough to show that $F_f' \in \mathcal{C}(\mathfrak{h}_1')$ and $f \to F_f'$ is a continuous mapping of $C_c^\infty(G)$ into $\mathcal{C}(\mathfrak{h}_1')$. But we have just seen that $F_f' = \zeta\phi_{\bar{f}}$, and therefore, in view of what has been said above, it is sufficient to prove that $\sigma: f \to \bar{f}$ is a continuous mapping of $C_c^\infty(G)$ into $C_c^\infty(\mathfrak{g}_0)$. Let ω be a bounded open subset of G. Since $C_c^\infty(\mathfrak{g}_0)$ is a locally convex space, it would be enough to prove that σ is continuous on $C_c^\infty(\omega)$ (see Schwartz [6, p. 69, Theorem II]). Let $\bar{\omega}$ denote the closure of ω and W the carrier of Φ. Then $W \subset V$, and it follows from Lemma 12 that $\exp W$ is closed in G. Hence $\bar{\omega} \cap \exp W$ is compact. Let Ω denote the complete inverse image of $\bar{\omega} \cap \exp W$ in V under the exponential mapping. Then by Lemma 11, Ω is also compact. Select an open neighborhood Ω_1 of Ω in $\mathfrak{g}_0$ such that its closure $\bar{\Omega}_1$ is compact and contained in V. Then for any $p \in S(\mathfrak{g})$, $\partial(p)\Phi$ remains bounded on Ω_1. Since the exponential mapping defines an analytic isomorphism of V with V_G, it is now clear that for any $q \in S(\mathfrak{g})$, we can choose a finite number of elements $b_1, \cdots, b_m \in \mathfrak{B}$ such that

$$|\bar{f}(X;\partial(q))| \leqq \sum_{1 \leqq i \leqq m} |f(\exp X; b_i)|$$

for all $f \in C_c^\infty(\omega)$ and $X \in \Omega_1$. But since $\bar{f}$ is zero (on $\mathfrak{g}_0$) outside Ω, this obviously implies that σ is continuous on $C_c^\infty(\omega)$. Hence the lemma is proved.

Now fix a point h_0 in A and let Ξ and $\mathfrak{z}_0$ be the centralizers of h_0 in G

---

[9] We are using here the notation of [4(h), § 5].

and $\mathfrak{g}_0$, respectively. Then as we have already seen in § 2, $\mathfrak{z}_0$ is reductive in $\mathfrak{g}_0$ and $\operatorname{rank} \mathfrak{z}_0 = \operatorname{rank} \mathfrak{g}_0$. Let Ξ_0 be the analytic subgroup of G corresponding to $\mathfrak{z}_0$. Then we know from Lemma 15 of [4(i)] that $\Xi/\Xi_0 Z$ is finite. Put $\bar{G} = G/\Xi$ and let $x \to \bar{x}$ ($x \in G$) denote the natural mapping G on $\bar{G}$. Since $\mathfrak{z}_0$ is reductive, there exists (see Weil [7, p. 45]) an invariant measure $d\bar{x}$ on $\bar{G}$. Similarly there exists a measure $d\xi^*$ on $\Xi^* = \Xi/A$ which is invariant under the operations of Ξ. It is well known (see Weil [7]) that $d\bar{x}$ and $d\xi^*$ can be so normalized that[1]

$$\int \gamma(x^*)\,dx^* = \int \bar{\gamma}(\bar{x})\,d\bar{x} \qquad (\gamma \in C_c(G^*)),$$

where

$$\bar{\gamma}(\bar{x}) = \int_{\Xi^*} \gamma(x\xi^*)\,d\xi^* \qquad (x \in G)$$

and $xy^* = (xy)^*$ ($x, y \in G$). Select an open, connected and bounded neighborhood B_0 of 1 in A_0 such that $B = h_0 B_0$ satisfies the condition of Theorem 1. We assume that B_0 is so small that $|\eta_\alpha(h) - 1| \geqq \frac{1}{2} |\eta_\alpha(h_0) - 1|$ for $h \in B$ and $\alpha \in P$. Let $\mathfrak{z}$ be the complexification of $\mathfrak{z}_0$ in $\mathfrak{g}$ and P_1 the set of all roots $\alpha \in P$ for which $X_\alpha \in \mathfrak{z}$. Also let P_2 the the complement of P_1 in P. Then if

$$\Delta_i' = \prod_{\alpha \in P_i} (1 - \eta_\alpha^{-1}) \qquad (i = 1, 2),$$

it is clear that Δ_2' is never zero on B and $\Delta'(h_0 h) = \Delta_1'(h)\Delta_2'(h_0 h)$ ($h \in B_0$). Hence $B_0' = h_0^{-1}(B \cap A')$ consists of all those $h \in B_0$ where $\Delta_1'(h) \neq 0$. Let Ξ_0^* denote the image of Ξ_0 in Ξ^* and put $\Xi_1 = \Xi_0 A$. Since Ξ_0 is normal in Ξ, Ξ_1 is a group and $\Xi_1 \supset \Xi_0 Z$. Therefore, in view of the finiteness of $\Xi/\Xi_0 Z$, we can select a finite number of elements $y_1 = 1, y_2, \cdots, y_r$ in Ξ such that Ξ is the disjoint union of the cosets $y_i \Xi_1$ ($1 \leqq i \leqq r$). Then Ξ^* is the disjoint union of the open sets $y_i \Xi_0^*$ ($1 \leqq i \leqq r$) and $\Xi_0^* \cong \Xi_0/\Xi_0 \cap A$. Since $\mathfrak{z}_0$ is reductive, Lemma 15 is obviously applicable to Ξ_0 in place of G. Moreover, $B_0 \subset \Xi_0$ since B_0 is connected. Put

$$\psi_g(h) = \Delta_1'(h) \int_{\Xi_0^*} g(h^{\xi^*})\,d\xi^* \qquad (h \in B_0')$$

for $g \in C_c^\infty(\Xi_0)$. Then if B_0 is chosen sufficiently small, it follows from Lemma 15 (applied to Ξ_0) that $\psi_g \in \mathscr{B}_0(B_0')$ and $g \to \psi_g$ is a continuous mapping of $C_c^\infty(\Xi_0)$ into $\mathscr{B}_0(B_0')$.

Now if $f \in C_c^\infty(G)$, it is clear that

$$\int_{G^*} f(h^{x^*})\,dx^* = \int_{\bar{G}} f(h : \bar{x})\,d\bar{x} \qquad (h \in B \cap A'),$$

where

$$f(h:\bar{x})=\int_{\Xi^*} f(xh^{\xi^*}x^{-1})\,d\xi^*=\sum_{1\leq i\leq r}\int_{\Xi_0^*} f(xy_ih^{\xi^*}y_i^{-1}x^{-1})\,d\xi^* \qquad (x\in G).$$

Let ω be a bounded open subset of G. Then it follows from our definition of B that there exists a compact set $\bar{\Omega}$ in $\bar{G}$ with the following property. If $xhx^{-1}\in\omega$ for some $x\in G$ and $h\in B$, then $\bar{x}\in\bar{\Omega}$. Let dx and $d\xi$ denote the Haar measures on G and Ξ, respectively. We normalize them in such a way that

$$\int_G \gamma(x)\,dx=\int_{\bar{G}}\gamma'(\bar{x})\,d\bar{x} \qquad (\gamma\in C_c(G))$$

where $\gamma'(\bar{x})=\int \gamma(x\xi)\,d\xi$ $(x\in G)$. Select a function $\alpha\in C_c(G)$ such that $\alpha'=1$ on $\bar{\Omega}$ and put

$$g_f(\xi)=\sum_{1\leq i\leq r}\int_G \alpha(x)f(xy_ih_0\xi y_i^{-1}x^{-1})\,dx \qquad (\xi\in\Xi_0)$$

for any $f\in C_c^\infty(\omega)$. Then it is clear that

$$\int_{G^*} f((h_0h)^{x^*})\,dx^*=\int_{\bar{\Omega}} f(h_0h:\bar{x})\,d\bar{x}=\int_{\Xi_0^*} g_f(h^{\xi^*})\,d\xi^* \qquad (h\in B_0')$$

for $f\in C_c^\infty(\omega)$. Put

$$\beta'(h)=\Delta_2'(h)\beta(h_0^{-1}h) \qquad (h\in B\cap A')$$

for $\beta\in\mathcal{B}_0(B_0')$. It is obvious that Δ_2' is bounded away from zero on B. Therefore $\beta\to\beta'$ is a continuous mapping of $\mathcal{B}_0(B_0')$ onto $\mathcal{B}(B\cap A')$. On the other hand, if $f\in C_c^\infty(\omega)$,

$$\begin{aligned}F_f(h_0h)&=\Delta'(h_0h)\int_{G^*} f((h_0h)^{x^*})\,dx^*\\&=\Delta_2'(h_0h)\psi_{g_f}(h) \qquad (h\in B_0'),\end{aligned}$$

and therefore $F_f=\psi_{g_f}'$ on $B\cap A'$. The mapping $f\to g_f$ of $C_c^\infty(\omega)$ into $C_c^\infty(\Xi_0)$ is obviously continuous. Therefore $f\to\psi_{g_f}'$ is a continuous mapping of $C_c^\infty(\omega)$ into $\mathcal{B}_0(B\cap A')$. Thus we have obtained the following improved version of Lemma 15.

LEMMA 16. *Let h_0 be a point in A. Then there exists an open neighborhood ${}_0A$ of h_0 in A with the following property. Put ${}_0A'={}_0A\cap A'$ and let ${}_0F_f$ denote the restriction of F_f on ${}_0A'$ $(f\in C_c^\infty(G))$. Then ${}_0F_f\in\mathcal{B}_0({}_0A')$ and $f\to{}_0F_f$ is a continuous mapping of $C_c^\infty(G)$ into $\mathcal{B}_0({}_0A')$.*

It is now easy to deduce Theorem 2. Let ω be a nonempty bounded open set in G. Define B as in Lemma 13. Then it follows from Lemma 16 and the boundedness of B that there exist a finite number of nonempty open subsets A_i of A $(1 \leqq i \leqq r)$ such that $B \subset \bigcup_{1 \leqq i \leqq r} A_i$ and the following conditions are fulfilled. Let ${}_iF_f$ denote the restriction of F_f on A_i for $f \in C_c^\infty(G)$. Then ${}_iF_f \in \mathcal{B}_0(A_i \cap A')$ and the mapping $f \to {}_iF_f$ of $C_c^\infty(G)$ into $\mathcal{B}_0(A_i \cap A')$ is continuous for every i. Now if $f \in C_c^\infty(\omega)$, F_f is zero on A' outside B. Hence it is clear that

$$\sup_{H \in A'} |F_f(H;v)| \leqq \sum_{1 \leqq i \leqq r} \sup_{H \in A'_i} |F_f(H;v)| \qquad (v \in \mathfrak{H}),$$

where $A_i' = A_i \cap A'$. Therefore it follows that $F_f \in \mathcal{B}_0(A')$ and the mapping $f \to F_f$ of $C_c^\infty(\omega)$ into $\mathcal{B}_0(A')$ is continuous. All the statements of Theorem 2 are now obvious.

The following lemma is an immediate consequence of Theorem 2. Let dh denote the Haar measure on A.

LEMMA 17. *Let g be a measurable function on A which is bounded on every compact set. Then the mapping*

$$f \to \int_A F_f(h) g(h) dh \qquad (f \in C_c^\infty(G))$$

is a distribution on G.

This holds in particular if g is a character of A.

5. The main theorems. Let $\mathfrak{Z}$ denote the center of $\mathfrak{B}$. Then from Lemma 18 of [4(c)] there exists an isomorphism γ' of $\mathfrak{Z}$ into $S(\mathfrak{h})$ such that

$$z - \partial(\gamma'(z)) \in \sum_{\alpha \in P} \mathfrak{B} X_\alpha \qquad (z \in \mathfrak{Z}).$$

THEOREM 3. *Define F_f as in Theorem 2. Then*

$$F_{zf} = \partial(\gamma'(z)) F_f$$

for $f \in C_c^\infty(G)$ and $z \in \mathfrak{Z}$.

Fix a point $h_0 \in A'$ and let ω be a bounded open subset of G. Then as we saw during the proof of Lemma 14, there exists an open connected neighborhood B of h_0 in A' and a compact set Ω_0^* in G^* with the following property. If $xhx^{-1} \in \omega$ for some $h \in B$ and $x \in G$, then $x^* \in \Omega_0^*$. Therefore

$$F_g(h) = \Delta'(h) \int_{\Omega_0^*} g(h^{x^*}) dx^* \qquad (h \in B, g \in C_c^\infty(\omega)).$$

Let Ω^* be a compact neighborhood of Ω_0^* in G^*. Normalize the Haar measures dx and dh on G and A, respectively, in such a way that

$$\int_G \beta(x)\,dx = \int_{G^*} dx^* \int_A \beta(xh)\,dh \qquad (\beta \in C_c(G)),$$

and select $\alpha \in C_c^\infty(G)$ such that $\int \alpha(xh)\,dh = 1$ if $x^* \in \Omega^*$ $(x \in G)$. Then if $f \in C_c^\infty(\omega)$ and $z \in \mathfrak{Z}$, it is obvious that

$$F_{zf}(h) = \Delta'(h) \int_G \alpha(x) f(xhx^{-1}; z)\,dx \qquad (h \in B).$$

Now we use the notation of [4(c), § 7] and put $f(x\colon h) = f(xhx^{-1})$ $(x \in G, h \in B)$. Then it follows from Lemma 23 of [4(c)] that

$$z = \Gamma_h(1 \times \beta_h(z)) + \sum_{1 \leqq i \leqq N} a_i(h) \Gamma_h(b_i \times u_i) \qquad (h \in B),$$

where $b_i \in \mathfrak{B}\mathfrak{g}, u_i \in \mathfrak{H}$ and a_i are analytic functions on B. Since $\mathfrak{B}\mathfrak{g}$ is the direct sum of $\mathfrak{S}'$ and $\mathfrak{B}\mathfrak{h}$ and $\Gamma_h(\mathfrak{B}\mathfrak{h} \times \mathfrak{H}) = \{0\}$, we may assume that $b_i \in \mathfrak{S}'$ and u_i $(1 \leqq i \leqq N)$ are linearly independent. Then since $z^h = z$, it follows from Lemma 22 of [4(c)] that $b_i^h = b_i$ $(h \in A)$. Therefore

$$f(xhx^{-1}; z) = f(x\colon h; \beta_h(z)) + \sum_{1 \leqq i \leqq N} a_i(h) f(x; b_i\colon h; u_i) \qquad (h \in B, x \in G)$$

and

$$F_{zf}(h) = \Delta'(h) \int_G \alpha(x) f(x\colon h; \beta_h(z))\,dx + \sum_{1 \leqq i \leqq N} a_i(h) \Delta'(h) \int_G \alpha(x; b_i^*) f(x\colon h; u_i)\,dx$$

for $h \in B$. (Here b_i^* is the adjoint of b_i). We now claim that

$$\int \alpha(x; b_i^*) f(x\colon h; u_i)\,dx = 0 \qquad (1 \leqq i \leqq N, h \in B).$$

It is clear that for a fixed $h, f(x\colon h; u_i)$ depends only on x^*. Hence it would be enough to prove that

$$\int_A \alpha(xh; b_i^*)\,dh = 0$$

if $x^* \in \Omega_0^*$. Choose a point $x_0 \in G$ such that $x_0^* \in \Omega_0^*$ and let U be an open neighborhood of 1 in G such that $(x_0 U)^* \subset \Omega^*$. Then it follows from the definition of α that

$$\int_A \alpha(x_0 yh)\,dh = 1 \qquad (y \in U).$$

Put $\alpha(x\colon h) = \alpha(xh)$ $(x \in G, h \in A)$. It is obvious that $(b_i^*)^h = b_i^*$ $(h \in A)$ and therefore $\alpha(x; b_i^*\colon h) = \alpha(xh; b_i^*)$. Therefore

$$\int_A \alpha(x_0 h; b_i^*)\, dh = \int_A \alpha(x_0; b_i^*\colon h)\, dh = 0$$

since $b_i^* \in \mathfrak{B}\mathfrak{g}$ and $\int \alpha(x_0 y\colon h)\, dh = 1$ for $y \in U$. This proves that

$$F_{zf}(h) = \Delta'(h) \int_G \alpha(x) f(x\colon h; \beta_h(z))\, dx \qquad (h \in B).$$

On the other hand, Theorem 2 of [4(c)] gives us a formula for $\beta_h(z)$. Define d as in this theorem. It follows easily from Lemma 7 of [4(c)] that $\operatorname{conj} \eta_\alpha(h^{-1}) = \eta_{\theta\alpha}(h)$ for $\alpha \in P$ and $h \in A$. Now if [9] $\alpha \in P_+$, the same holds for $-\theta\alpha$. Hence if $P' = P_0 \cup P_-$ (see [4(h), § 5] for notation), it is clear that

$$\operatorname{conj} \Delta'(h) = \prod_{\alpha \in P} (1 - \eta_{\theta\alpha}(h)) = (-1)^{r'} \prod_{\alpha \in P'} \eta_\alpha(h) \Delta'(h) \qquad (h \in A),$$

where r' is the number of roots in P'. Therefore

$$\begin{aligned} |d(h)| &= \Big| \prod_{\alpha \in P} (\eta_\alpha(h^{-1}) - 1)(\eta_\alpha(h) - 1) \Big| \\ &= \Big| \prod_{\alpha \in P_+} \eta_\alpha(h) \Big| \, |\Delta'(h)|^2 = (-1)^{r'} \Big| \prod_{\alpha \in P_+} \eta_\alpha(h) \Big| \prod_{\alpha \in P'} \eta_\alpha(h) \Delta'(h)^2. \end{aligned}$$

But

$$\operatorname{conj} \prod_{\alpha \in P_+} \eta_\alpha(h) = \prod_{\alpha \in P_+} \eta_{\theta\alpha}(h^{-1}) = \prod_{\alpha \in P_+} \eta_\alpha(h),$$

and so

$$|d(h)| = \pm \prod_{\alpha \in P} \eta_\alpha(h) \Delta'(h)^2.$$

Put $\rho = \frac{1}{2} \sum_{\alpha \in P} \alpha$ and select an open connected neighborhood $\mathfrak{h}_1$ of zero in $\mathfrak{h}_0$ such that $B_1 = h_0 \exp \mathfrak{h}_1 \subset B$. Then it is clear that

$$|d(h_0 \exp H)|^{\frac{1}{2}} = \epsilon e^{\rho(H)} \Delta'(h_0 \exp H) \qquad (H \in \mathfrak{h}_1),$$

where ϵ is a constant such that $\epsilon^4 = 1$. Therefore, it follows from Theorem 2 of [4(c)] that $\beta(z) = (\Delta')^{-1} \partial(\gamma'(z)) \circ \Delta'$ on B_1 and so

$$\begin{aligned} F_{zf}(h) &= \int \alpha(x) f(x\colon h; \partial(\gamma'(z)) \circ \Delta')\, dx \\ &= F_f(h; \partial(\gamma'(z))) \qquad (h \in B_1). \end{aligned}$$

This proves that F_{zf} and $\partial(\gamma'(z)) F_f$ coincide at h_0, and hence the theorem is established.

Put

$$\Delta_+'(h)=\prod_{\alpha\in P_+}(1-\eta_\alpha(h^{-1})),\qquad \Delta_0'(h)=\prod_{\alpha\in P_0}(1-\eta_\alpha(h^{-1}))\qquad (h\in A).$$

Then $\Delta_+'(h)$ is real since

$$\operatorname{conj}\Delta_+'(h)=\prod_{\alpha\in P_+}(1-\eta_{\bar\alpha}(h))=\prod_{\alpha\in P_+}(1-\eta_\alpha(h^{-1}))=\Delta_+'(h)$$

LEMMA 18. *Let $\epsilon_+(h)$ $(h\in A')$ denote the sign of $\Delta_+'(h)$ and A'' the set of all points $h\in A$ where $\Delta_0'(h)\neq 0$. Then for any $f\in C_c^\infty(G)$, ϵ_+F_f can be extended to a function of class C^∞ on A''.*

We use the notation of the proof of Lemma 15. Then

$$F_f(\exp H)=\zeta(H)\phi_f(H)\qquad (H\in\mathfrak{h}_1').$$

Put $\pi_+=\prod_{\alpha\in P_+}\alpha\in S(\mathfrak{h})$. It is obvious that if $\mathfrak{h}_1$ is sufficiently small, $\Delta_+'(\exp H)/\pi_+(H)$ can be extended to an analytic function on $\mathfrak{h}_1$ which is nowhere zero and which takes the value 1 at $H=0$. Therefore, since $\pi_+(H)$ is also real for $H\in\mathfrak{h}_0$, it has the same sign as $\Delta_+'(\exp H)$ for $H\in\mathfrak{h}_1'$. Hence it follows from Theorem 3 of [4(h)] that ϵ_+F_f can be extended to a function of class C^∞ on $B\cap A''$, where $B=\exp\mathfrak{h}_1$.

Now h_0 being a fixed point in A'', we use the notation of the proof of Lemma 16. Then $F_f=\psi_{g_f}'$ on $B\cap A'$. Since Δ_2' is never zero on B, it is clear that ϵ_+ differs on B from the sign of

$$\prod_{\alpha\in P_1\cap P_+}(1-\eta_\alpha(h^{-1}))$$

only by a constant factor. Therefore, by applying the above result to Ξ_0, we can conclude that there exists an open neighborhood B_1 of h_0 in B such that $\epsilon_+\psi_{g_f}'$ can be extended to a function of class C^∞ on $B_1\cap A''$. Since $\epsilon_+F_f=\epsilon_+\psi_{g_f}'$ on $B_1\cap A'$ and A' is dense in A'', the assertion of the lemma is now obvious.

Define $\mathfrak{h}_1$ and ζ as in the proof of Lemma 15 and put[8] $\pi'=\prod_{\alpha\in P}\{\alpha+\langle\alpha,\rho\rangle\}$ and consider the differential operator $\partial(\pi')\circ\zeta$ on $\mathfrak{h}_1$. As usual we denote its local expression at zero by $(\partial(\pi')\circ\zeta)_0$.

LEMMA 19. $(\partial(\pi')\circ\zeta)_0=\partial(\pi)$.

Since

$$\Delta'(\exp H)=e^{-\rho(H)}\prod_{\alpha\in P}(e^{\alpha(H)/2}-e^{-\alpha(H)/2})\qquad (H\in\mathfrak{h}_1)$$

and $e^{\rho}\partial(\pi')\circ e^{-\rho}=\partial(\pi)$, it would be enough to prove that $(\partial(\pi)\circ\zeta_1)_0=\partial(\pi)$, where

$$\zeta_1(H)=\prod_{\alpha\in P}g(\alpha(H)) \qquad (H\in\mathfrak{h}_1)$$

and g denotes the entire function $(e^{t/2}-e^{-t/2})/t$ of the complex variable t. Then

$$\zeta_1=1+\sum_{k\geqq 1}p_k,$$

where p_k is a homogeneous polynomial in $S(\mathfrak{h})$ of degree k and the above series converges to ζ_1 in some neighborhood $\mathfrak{h}_2$ of zero in $\mathfrak{h}_1$. Let W be the Weyl group of $\mathfrak{g}$ with respect to $\mathfrak{h}$. Then ζ_1 can be regarded as a holomorphic function on some complex neighborhood U of zero in $\mathfrak{h}$, and we may assume that $sU=U$ $(s\in W)$ and the above series converges to ζ_1 on U. Then since $\zeta_1(sH)=\zeta_1(H)$ $(s\in W)$, it follows that $p_k^s=p_k$ $(s\in W, k\geqq 1)$. Moreover, if f is any homogeneous element in $S(\mathfrak{h})$, it is obvious that

$$f(0;\partial(\pi)\circ\zeta_1)=f(0;\partial(\pi))+\sum_{1\leqq k\leqq r}f(0;\partial(\pi)\circ p_k),$$

where r is the degree of π. But it follows from Lemma 18 of [4(g)] that $f(0;\partial(\pi)\circ p_k)=0$, and so $f(0;\partial(\pi)\circ\zeta_1)=f(0;\partial(\pi))$. Hence, if $(\partial(\pi)\circ\zeta_1)_0-\partial(\pi)=\partial(q)$ $(q\in S(\mathfrak{h}))$, then[8] $\langle p,q\rangle=0$ for all $p\in S(\mathfrak{h})$, and therefore (see [4(g), § 2]) $q=0$. This proves the assertion of the lemma.

We say that the Cartan subgroup A is fundamental if $\mathfrak{h}_0$ is fundamental in $\mathfrak{g}_0$ (see [4(h), § 8]).

THEOREM 4. *We can select a neighborhood B of 1 in A with the following property. Suppose A_1 is a connected component of $A'\cap B$ whose closure contains 1. Then there exists a real number c such that*

$$\operatorname{Lim}_{h\to 1}F_f(zh;\partial(\pi'))=cf(z) \qquad (h\in A_1)$$

for all $f\in C_c^\infty(G)$ and $z\in Z$. Moreover, $c=0$ if A is not fundamental.

If $z=1$, our statement is an immediate consequence of Lemma 19 and the fact that

$$F_f(\exp H)=\zeta(H)\phi_{\bar f}(H) \qquad (H\in\mathfrak{h}_1'),$$

if we take into account Theorem 2 of [4(i)]. For any arbitrary $z\in Z$, write $f_z(x)=f(zx)$ $(x\in G)$. Then

$$\operatorname{Lim}_{h\to 1}F_f(zh;\partial(\pi'))=\operatorname{Lim}_{h\to 1}F_{f_z}(h;\partial(\pi'))=cf_z(1)=cf(z) \qquad (h\in A_1).$$

THEOREM 5. *Suppose A is fundamental and $A_1, A_2,\cdots, A_r$ are all*

the distinct connected components of $A' \cap B$ *whose closures contain* 1. *Let* c_i *be the real number of Theorem* 4 *corresponding to* A_i. *Then* $c_1 + c_2 + \cdots + c_r \neq 0$.

This follows immediately from Theorem 3 of [4(i)].

Note added on August 3, 1957. Recently I have been able to prove that $c_1 = c_2 = \cdots = c_r$ in Theorem 5. Since the normalization of the measure dx^* in Theorem 2 is arbitrary, only the sign of c_1 is of interest. Assuming that $\mathfrak{h}_0$ is fundamental, let p_+ and p_0 denote the number of roots in P_+ and P_0, respectively. Then p_+ is even and, if $q = p_0 + \frac{1}{2}p_+$, the sign of c_1 is $(-1)^q$.

COLUMBIA UNIVERSITY,
NEW YORK, N. Y.

REFERENCES.

[1] G. Birkhoff, *Ann. of Math.*, vol. 38 (1937), pp. 526-532.

[2] C. Chevalley, (a) *Theory of Lie Groups*, Princeton University Press, 1946.
(b) *Amer. Jour. Math.*, vol. 63 (1941), pp. 785-793.

[3] I. M. Gelfand and M. I. Graev, *Doklady Akad. Nauk. SSSR N. S.*, vol. 92 (1953), pp. 461-464.

[4] Harish-Chandra, (a) *Trans. Amer. Math. Soc.*, vol. 76 (1954), pp. 234-253.
(b) ———, vol. 76 (1954), pp. 485-528.
(c) ———, vol. 83 (1956), pp. 98-163.
(d) *Amer. Jour. Math.*, vol. 77 (1955), pp. 743-777.
(e) ———, vol. 78 (1956), pp. 1-41.
(f) ———, vol. 78 (1956), pp. 564-628.
(g) ———, vol. 79 (1957), pp. 87-120.
(h) ———, vol. 79 (1957), pp. 193-257.
(i) ———, vol. 79 (1957), pp. 653-686.
(j) *Proc. Nat. Acad. Sci. U.S.A.*, vol. 42 (1956), pp. 538-540.

[5] K. Iwasawa, *Ann. of Math.*, vol. 50 (1949), pp. 507-557.

[6] L. Schwartz, *Theorie des distributions I*, (1950), Paris, Hermann.

[7] A. Weil, *L'integration dans les groupes topologiques et ses applications*, Paris, Hermann.

DIVISORS AND ENDOMORPHISMS ON AN ABELIAN VARIETY.*

By Serge Lang.

We consider here the fundamental theorem on the algebra of endomorphisms of an abelian variety dealing with the existence of a positive definite quadratic form defined by means of the trace. We shall give a direct proof on abelian varieties for Weil's formula $\sigma(\xi\xi') > 0$, which will exhibit the positivity as a formal consequence of the definitions. Weil's method is to show that the trace can be expressed as an intersection number (Proposition 20 of [6], No. 47). However, even on a Jacobian, his proof that $\sigma(\xi)$ coincides with the penultimate coefficient of the characteristic polynomial is somewhat indirect (Theorem 34 of [6], No. 66). In the present exposition, this will be straightforward, and we shall obtain a simple representation of the trace as an intersection number canonically determined by a given projective embedding of the abelian variety A, or as Weil would say, a polarization of A [8].

More generally, if α_i $(i=1,\cdot\cdot\cdot,d)$ are endomorphisms of A and m_i $(i=1,\cdot\cdot\cdot,d)$ are integers, then we give an expression for the coefficients of the homogeneous polynomial $\nu(m_1\alpha_1+\cdot\cdot\cdot+m_d\alpha_d)$ in terms of intersection numbers canonically determined by the α_i and the given polarization.

Our arguments are based on only two properties of abelian varieties: The theorem of the square (see below), and the fact that a divisor which is $\equiv 0$ is numerically equivalent to 0. (Weil [6], No. 62 and Morikawa [5], Lemma 7.) For the convenience of the reader, we reproduce in an appendix a simple proof of Weil for this fact.

We shall begin by defining a bilinear mapping of the endomorphisms of A into the Neron-Severi group of divisors $N(A)$, given by the formula $D_X(\alpha,\beta)\equiv(\alpha+\beta)^{-1}(X)-\alpha^{-1}(X)-\beta^{-1}(X)$. The properties of the trace are then reflected from analogous properties of our divisorial pairing. We shall take X to be a positive non-degenerate divisor. We call a class of divisors in $N(A)$ positive if a suitable positive integral multiple of it contains a positive divisor. The formula $\operatorname{tr}(\alpha\alpha')>0$ then comes from the fact that $D_X(\alpha,\alpha)$ is positive.

We then discuss a pairing of endomorphisms into the group $N_1(A)$ of

* Received February 15, 1957.

4

1-cycles modulo those which are numerically equivalent to 0. It is dual to the above, and is defined by the formula $Z_C(\alpha,\beta) = (\alpha+\beta)(C) - \alpha(C) - \beta(C)$. Properties of $D_X(\alpha,\beta)$ are easily transferred to properties of $Z_C(\alpha,\beta)$. We introduce the Pontrjagin product between cycles of A, which is dual to the intersection product, and are then able to recover all the numerical statements contained in Weil [6] (for instance, the Lefschetz fixed point formula for curves). Some questions concerning the Pontrjagin product remain unanswered, principally those concerning the more precise duality which exists between this product and the ordinary intersection product.

The above section dealing with 1-cycles is not used in the section following it, where we analyse the positivity of divisor classes in $N(A)$. We generalize results of Morikawa [5], except that we work only in the tensor product of $N(A)$ with the rational numbers, and do not consider integrality questions related to the positivity. For instance, let Y be a divisor and suppose that there exists an integer $m > 0$ and a divisor $Y_1 > 0$ such that $mY \equiv Y_1$. Does there exist a divisor $Y_2 > 0$ such that $Y \equiv Y_2$?

Finally, we have pointed out how one can see directly on an abelian variety that the characteristic roots of the Frobenius endomorphism all have absolute value $q^{\frac{1}{2}}$ without having to go through the theory of curves. Together with the Lefschetz fixed point formula, this gives a more natural proof for the Riemann hypothesis for curves.

1. Applications of the theorem of the square. For the rest of this paper, A, B will denote abelian varieties and $X, Y, Z, \cdots$ will be divisors on A or B. We denote by $H(A,B)$ the module of homomorphisms of A into B, and by $H(A)$ the ring of endomorphisms of A. The tensor products with $\boldsymbol{Q}$ will be denoted by $H_{\boldsymbol{Q}}(A,B)$ and $H_{\boldsymbol{Q}}(A)$ respectively. If $\alpha \in H_{\boldsymbol{Q}}(A,B)$ and $\nu(\alpha) \neq 0$, then there is an element β of $H_{\boldsymbol{Q}}(B,A)$ such that $\beta\alpha$ is the identity. We write $\beta = \alpha^{-1}$.

We denote by $\hat{A}$ the dual variety (Picard variety) of A. If X is a divisor on A, algebraically equivalent to 0, then $\mathrm{Cl}(X)$ denotes the point on $\hat{A}$ associated with the linear equivalence class of X. The theorem of the square states that the mapping

$$\varphi_X : u \to \mathrm{Cl}(X_u - X)$$

is a homomorphism of A into $\hat{A}$. By definition, $X \equiv 0$ if and only if $\varphi_X = 0$.

We let $D(A)$ be the group of divisors on A, and $D_l(A)$ the subgroup of divisors linearly equivalent to 0. Let $\alpha \in H(A,B)$. Let X be a divisor on B. Then $\alpha^{-1}(X)$ may not be defined, but if t is a generic point of B.

then $\alpha^{-1}(X_t)$ is always defined. Furthermore, if X is algebraically equivalent to 0 on B, then $X_t \sim X$, and if $X \sim 0$ on B and $\alpha^{-1}(X)$ is defined, then $\alpha^{-1}(X) \sim 0$ on A. If V is a variety, we denote by $D_a(V)$ the group of divisors algebraically equivalent to 0 on V. Then the above remarks show that α induces a linear map α^{-1} of $D_a(B)/D_l(B)$ into $D_a(A)/D_l(A)$. (Later we shall use the terminology of the Picard variety, and we call this map the transpose of α.)

We denote by $N(A)$ the factor group of $D(A)$ by the subgroup of divisors of A which are $\equiv 0$. Then α will also induce an inverse mapping α^{-1} of $N(B)$ into $N(A)$ as follows. We contend that if t and u are generic points of B then $\alpha^{-1}(X_t) \equiv \alpha^{-1}(X_u)$. To prove this, we first state a lemma explicitly.

Lemma. *Let $\lambda\colon A \to B$ be a homomorphism, X a divisor on B, v a point of A such that $\lambda^{-1}(X_{\lambda v})$ is defined. Assume also that $\lambda^{-1}(X)$ is defined. Then $(\lambda^{-1}(X))_v = \lambda^{-1}(X_{\lambda v})$.*

Proof. The translation $(v, \lambda v)$ on $A \times B$ leaves the graph of λ fixed. It moves $\lambda^{-1}(X)$ on its translate by v, and moves X on its translate by λv. The lemma is then obvious.

Returning to the proof of our contention, we let v be a generic point of A, independent of t and u. Then $\alpha^{-1}(X_{t+\alpha v})$ and $\alpha^{-1}(X_{u+\alpha v})$ are defined, and a trivial computation starting with the definitions, together with the theorem of the square proves our contention.

Given a divisor X on B, and $\alpha \in H(A,B)$, then from the theorem of the square, we know that $X_t \equiv X$, and hence the class $\alpha^{-1}(X_t)$ in $N(A)$ depends only on X and α and not on the auxiliary generic point t. By an abuse of language, we shall denote this class by $\alpha^{-1}(X)$. The context will always make clear whether we deal with a class in $N(A)$, or whether we deal with a divisor X in $D_a(B)$, in which case $\alpha^{-1}(X)$ will mean the linear equivalence class in $D_a(A)/D_l(A)$.

The following theorem and its proof are directly inspired from Weil's Proposition 31, [6], No. 73. For the special case of elliptic curves, see Hasse [4].

Theorem 1. *Let $\alpha, \beta \in H(A,B)$. Define*

$$D_X(\alpha, \beta) \equiv (\alpha + \beta)^{-1}(X) - \alpha^{-1}(X) - \beta^{-1}(X),$$

this being an element of $N(A)$. Let m, n be integers. Then

$$(m\alpha + n\beta)^{-1}(X) \equiv m^2\alpha^{-1}(X) + mnD_X(\alpha, \beta) + n^2\beta^{-1}(X).$$

Proof. The proof will be carried out in three steps. Throughout, we let $s_n\colon B\times\cdots\times B\to B$ be the sum on the product of B n-times with itself, and we let $p_i\colon B\times\cdots\times B\to B$ be the projection on the i-th factor.

1.) $X\equiv 0$ if and only if $s_n^{-1}(X)\sim\sum p_i^{-1}(X)$.

For simplicity take $n=2$. Then for u generic on B, we have

$$s_2^{-1}(X)\cdot(B\times u)=X_{-u}\times u.$$

Hence $[s_2^{-1}(X)-(X\times B)]$. $(B\times u)=(X_{-u}-X)\times u$. If $X\equiv 0$, then this is linearly equivalent to 0, and hence we can write

$$s_2^{-1}(X)\sim(X\times B)+(B\times Y)$$

for some divisor Y on B. By symmetry, we must have $Y\sim X$. The converse is equally clear.

2.) If $X\equiv 0$ then

$$(\alpha+\beta)^{-1}(X)\sim\alpha^{-1}(X)+\beta^{-1}(X).$$

Let $\lambda\colon A\to B\times B$ be the composite map (α,β), so we have $\lambda u=(\alpha u,\beta u)$ for u in A. Then $s_2\lambda=\alpha+\beta$, and $p_i\lambda=\alpha$ or β according as $i=1$ or 2. Using the formula $(fg)^{-1}=g^{-1}f^{-1}$ which is applicable in the present case, together with step 1, we get what we want.

3.) We finish the proof in this step. Let X be arbitrary. Using the above lemma, we get

$$((m\alpha+n\beta)^{-1}(X))_u-(m\alpha+n\beta)^{-1}(X)=(m\alpha+n\beta)^{-1}(X_{(m\alpha+n\beta)u}-X).$$

For any $v\in B$, $X_v-X\equiv 0$. Using step 2 and making repeated use of the theorem of the square, we see that this expression is linearly equivalent to

$$(1)\qquad m^2\alpha^{-1}(X_{\alpha u}-X)+mn\alpha^{-1}(X_{\beta u}-X)$$
$$+mn\beta^{-1}(X_{\alpha u}-X)+n^2\beta^{-1}(X_{\beta u}-X).$$

Let $Z=\alpha^{-1}(X_{\beta u}-X)+\beta^{-1}(X_{\alpha u}-X)$. To prove our theorem, it suffices to shrow that $Z\sim D_X(\alpha,\beta)_u-D_X(\alpha,\beta)$. One sees this by putting $m=n=1$ in formula (1), and using the lemma.

To go further, it is convenient to use the language and formalism of the Picard variety. (At present, a complete exposition is not yet published. Some of it will be in Chow [3], and the commutative diagrams below are due to Weil. See also Morikawa [5].) Given a homomorphism $\alpha\in H(A,B)$, then one has an induced contravariant mapping on the Picard varieties.

${}^t\alpha\colon \hat{B} \to \hat{A}$, which we shall call the *transpose* of α. We shall use constantly the linearity property

$$(2) \qquad {}^t(\alpha+\beta) = {}^t\alpha + {}^t\beta,$$

which is essentially step 2 in the proof of Theorem 1. If $\theta_A\colon A \to \hat{\hat{A}}$ denotes the canonical map of A onto its double dual, and X is a divisor on A, then the following diagram is commutative:

$$(3) \qquad \begin{tikzcd} A \arrow[rr, "\varphi_X"] \arrow[dr, "\theta_A"'] & & \hat{A} \\ & \hat{\hat{A}} \arrow[ur, "{}^t\varphi_X"'] & \end{tikzcd}$$

If $\alpha \in H(A,B)$ and if Y is a divisor on B, then the following diagram is commutative:

$$(4) \qquad \begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\varphi_{\alpha^{-1}(Y)}"'] & B \arrow[d, "\varphi_Y"] \\ \hat{A} & \hat{B} \arrow[l, "{}^t\alpha"] \end{tikzcd}$$

i.e., we have $\varphi_{\alpha^{-1}(Y)} = {}^t\alpha \circ \varphi_Y \circ \alpha$.

It follows just as in Theorem 1 that

$$(5) \qquad \varphi_{D_X(\alpha,\beta)} = {}^t\alpha \circ \varphi_X \circ \beta + {}^t\beta \circ \varphi_X \circ \alpha$$

for any divisor X on B. Conversely, one might also use the present formalism to deduce the following generalization. If $\alpha_1, \cdots, \alpha_d$ are homomorphisms of A into B, and $m_1, \cdots, m_d$ are integers, then

$$(6) \qquad (m_1\alpha_1 + \cdots + m_d\alpha_d)^{-1}(X) \equiv \tfrac{1}{2} \sum m_i m_j D_X(\alpha_i, \alpha_j),$$

the sum being taken for $i, j = 1, \cdots, d$, so that each term appears twice and we therefore divide by 2.

In addition, the linearity property of the transpose gives us immediately a bilinear map of $H(A,B)$ into $N(A)$, namely the class of $D_X(\alpha,\beta)$ obeys the rules:

D1. $\qquad D_X(\alpha+\beta,\gamma) \equiv D_X(\alpha,\gamma) + D_X(\beta,\gamma).$

D2. $\qquad D_X(\alpha,\beta) \equiv D_X(\beta,\alpha).$

D3. $$D_X(m\alpha, \beta) \equiv mD_X(\alpha, \beta).$$

D4. $$D_X(\alpha, \alpha) \equiv 2\alpha^{-1}(X).$$

Condition D4 is due to the commutative diagram (4). The others are clear.

For the rest of this paper, we shall take $B = A$. Following Morikawa [5], we say that a divisor X on A is *non-degenerate* if the kernel of φ_X is finite. As Weil has shown [7], it is practically obvious that if X is positive and non-degenerate, then a suitable positive multiple of X is ample, i.e., becomes a hyperplane section in a projective embedding of A. From now on, *X will denote a positive non-degenerate divisor on A, whose class in $N(A)$ will remain fixed throughout.* It then follows that for any $\alpha \neq 0$ in $H(A)$, there exists an integer $m > 0$ and a divisor $Y > 0$ such that $m\alpha^{-1}(X) \equiv Y$. Condition D4 can thus be interpreted as a condition of positive definiteness.

Relative to our divisor X, we define an involution on $H_{\boldsymbol{Q}}(A)$ by letting $\alpha' = \varphi_X^{-1} \circ {}^t\alpha \circ \varphi_X$. The commutativity relations (3) and (4) show that $\alpha \to \alpha'$ is an anti-automorphism, i.e., that

$$(\alpha + \beta)' = \alpha' + \beta', \qquad (\alpha')' = \alpha, \qquad (\alpha\beta)' = \beta'\alpha', \qquad \delta' = \delta.$$

Our pairing $D_X(\alpha, \beta)$ in $N(A)$ can then be extended to a bilinear map of $H_{\boldsymbol{Q}}(A)$ into $N_{\boldsymbol{Q}}(A)$. We can rewrite formula (5) in the form

(7) $$\varphi_{D_X(\alpha,\beta)} = \varphi_X(\alpha'\beta + \beta'\alpha).$$

It will be convenient to introduce still another symbol. We define

$$D_X(\alpha) \equiv D_X(\alpha, \delta) \equiv (\alpha + \delta)^{-1}(X) - \alpha^{-1}(X) - X.$$

If $\alpha \in H(A)$, then $\alpha \to D_X(\alpha)$ gives a linear map of $H(A)$ into $N(A)$ which can be extended to a $\boldsymbol{Q}$-linear map of $H_{\boldsymbol{Q}}(A)$ into $N_{\boldsymbol{Q}}(A)$.

We can supplement D1-D4 by more formulas which give the behavior of our pairing under multiplication, namely, for any divisor Y, we have

D5. $$D_X(\varphi_X^{-1}\, {}^t\alpha\varphi_Y\beta) \equiv D_Y(\alpha, \beta).$$

D6. $$D_X(\lambda\alpha, \lambda\beta) \equiv D_{\lambda^{-1}(X)}(\alpha, \beta).$$

D7. $$D_X(\alpha\lambda, \beta\lambda) \equiv \lambda^{-1}D_X(\alpha, \beta).$$

These formulas are direct consequences of the definitions and commutativity.

From D5 we deduce immediately formulas for $D_X(\alpha)$, namely,

D8. $$D_X(\alpha, \beta) \equiv D_X(\alpha'\beta).$$

D9. $$D_X(\alpha\beta, \gamma) \equiv D_X(\beta, \alpha'\gamma).$$

D10. $$D_X(\beta'\alpha\beta) \equiv \beta^{-1}D_X(\alpha).$$

D11. $$D_X(\alpha) \equiv D_X(\alpha').$$

The preceding formulas exhaust the formal behavior of our divisorial pairing, and we shall now turn to its application to the trace.

2. The trace. In this section, we use as our basic fact that if $X \equiv 0$, then X is numerically equivalent to 0. In an appendix, we shall reproduce a simple proof due to Weil, based only on the theorem of the square.

We consider divisors up to numerical equivalence, since we are concerned here with numerical statements. If Y is a divisor on A, then the intersection of Y with itself s times is understood to be up to numerical equivalence. If $t_1, \cdots, t_s$ are independent generic points, then $Y_{t_1} \cdot Y_{t_2} \cdots Y_{t_s}$ is an element of that class, for instance. We let r be the dimension of A. If C is any positive cycle of dimension 1 on A, then $\deg(X \cdot C) > 0$ because we have assumed X positive non-degenerate, hence essentially a hyperplane section of A.

In what follows, we shall also use the formula

$$\alpha^{-1}(Y_1 \cdot Y_2) = \alpha^{-1}(Y_1) \cdot \alpha^{-1}(Y_2),$$

which holds whenever both sides are defined. Generic translations will always insure that this is the case. Note also if $\mathfrak{a}$ is a 0-cycle, and $\nu(\alpha) \neq 0$, then

$$\deg(\alpha^{-1}(\mathfrak{a})) = \nu(\alpha)\deg(\mathfrak{a}).$$

From these remarks, we first note that if we intersect both sides of (6) with themselves r times ($r = \dim A$), then we recover immediately Weil's theorem that $\nu(m_1\alpha_1 + \cdots + m_d\alpha_d)$ as a function of $(m_1, \cdots, m_d)$ is a homogeneous polynomial of degree $2r$. Moreover, its coefficients are easily determined explicitly in terms of intersections of the $D_X(\alpha_i, \alpha_j)$.

We are particularly interested in the special case which yields the characteristic polynomial of an endomorphism. In Theorem 1 we take $m = 1$, and $\beta = \delta$. We get:

$$(\alpha + n\delta)^{-1}(X) \equiv n^2X + nD_X(\alpha) + \alpha^{-1}(X).$$

Again raising this equation to the r-th power, we get

$$\nu(\alpha + n\delta)\deg(X^{(r)}) = c_{2r}n^{2r} + c_{2r-1}n^{2r-1} + \cdots + c_0,$$

where $X^{(r)}$ denotes the class up to numerical equivalence of the intersection of X with itself r times, and the c_i are integers which are easily determined

explicitly in terms of intersections of $\alpha^{-1}(X)$, X, and $D_X(\alpha)$. For instance, we have

$$c_{2r} = \deg X^{(r)}, \qquad c_{2r-1} = r\cdot\deg(X^{(r-1)}\cdot D_X(\alpha)), \qquad c_0 = \nu(\alpha)\deg X^{(r)}.$$

This shows that $\nu(\alpha + n\delta)$ is a polynomial in n with rational coefficients. In [6], No. 67-68, Weil gives a simple and direct argument showing that the characteristic polynomial is actually that obtained from an l-adic representation.

The trace of α, which we denote by $\mathrm{tr}(\alpha)$, is defined by the formula

$$\mathrm{tr}(\alpha) = r/\deg(X^{(r)})\cdot\deg(X^{(r-1)}\cdot D_X(\alpha)).$$

From D5 we immediately get

$$\mathrm{tr}(\alpha'\beta) = r/\deg(X^{(r)})\cdot\deg(X^{(r-1)}\cdot D_X(\alpha,\beta)).$$

The main properties of the trace are then directly traceable to the properties of the divisor class $D_X(\alpha,\beta)$.

On the algebra $H_{\boldsymbol{Q}}(A)$ over the rational numbers, we can define a scalar product (taking its value in $\boldsymbol{Q}$) by putting $(\alpha,\beta) = \mathrm{tr}(\alpha'\beta)$. We then have the usual properties of a bilinear form, whose quadratic form is positive definite, and in addition we have the multiplicative property $(\alpha\beta,\gamma) = (\beta,\alpha'\gamma)$. This follows immediately from the analogous properties of $D_X(\alpha,\beta)$. The strict positivity comes from the fact that for some integer $m > 0$, mX is a hyperplane section of A, and hence the class of $m\alpha^{-1}(X)$ in $N(A)$ contains a divisor $Y > 0$. As we have noted before, we must then have $\deg(X^{(r-1)}\cdot\alpha^{-1}(X)) > 0$. From D4 and the definition of (α,α) we conclude that $(\alpha,\alpha) > 0$.

We define the norm $\|\alpha\|$ as usual by $(\alpha,\alpha)^{\frac{1}{2}}$. Aside from the usual properties of a metric, we have in addition the following statements:

N1. $\|\alpha\| = \|\alpha'\|$

N2. $\|\alpha'\alpha\| = \|\alpha\alpha'\|$

N3. If $\alpha \neq 0$ and $\beta \neq 0$, then $\|\alpha\beta\| < \|\alpha\|\,\|\beta\|$.

The first two are clear from the commutativity of the trace. As to the third, we have

$$\|\alpha\beta\|^2 = \mathrm{tr}(\beta'\alpha'\alpha\beta) = \mathrm{tr}(\alpha'\alpha\beta\beta') = (\alpha'\alpha,\beta\beta') \leqq \|\alpha'\alpha\|\,\|\beta\beta'\|,$$

this last inequality being the Schwartz inequality. We are therefore reduced to proving the inequality $\|\alpha'\alpha\| < \|\alpha\|^2$. By definition we have $\|\alpha'\alpha\|^2 = \mathrm{tr}(\alpha'\alpha\alpha'\alpha) = \mathrm{tr}((\alpha\alpha')^2)$. Let ω_j be the characteristic roots of $\alpha\alpha'$. Then

ω_j^2 are the characteristic roots of $(\alpha\alpha')^2$. It is known, and we shall recall the proof in the next section, that the ω_j are totally real totally positive algebraic numbers. Our inequality is equivalent to $\sum \omega_j^2 < (\sum \omega_j)^2$ which is true in view of this fact.

As an application, we consider an abelian variety A defined over a finite field k with q elements, and assume that X is rational over k. Then one verifies trivially that if π is the Frobenius endomorphism relative to k, then $\pi\pi' = \pi'\pi = q\delta$. Hence in that case, $\| \pi \| = (2rq)^{\frac{1}{2}}$. Furthermore, $\operatorname{tr}(\pi) = \operatorname{tr}(\pi\delta) = (\pi, \delta)$ and by the Schwartz inequality we get

$$| \operatorname{tr}(\pi) | \leqq \| \pi \| \, \| \delta \| = 2rq^{\frac{1}{2}}.$$

For any integer n, we get $| \operatorname{tr}(\pi^n) | \leqq 2rq^{n/2}$. If ω_j are the characteristic roots of π, then ω_j^n are those of π^n. From this one sees easily that the absolute value of a characteristic root can be at most $q^{\frac{1}{2}}$. Since we have $\nu(\pi) = q^r$, the product of the characteristic roots of π must be equal to $\pm q^r$ Hence the absolute value of each one of the characteristic roots is exactly $q^{\frac{1}{2}}$.

3. A dual pairing.* We introduce a pairing of the endomorphisms of A into the group of 1-cycles on A modulo numerical equivalence which is dual to the divisorial pairing of Section 1. The symbol $\equiv$ will now denote numerical equivalence, and $N_i(A)$ denotes the factor group of i-cycles by those which are numerically equivalent to 0.

Let Z be a cycle on A. Let $\alpha \in H(A)$. As usual, we mean by $\alpha(Z)$ the intersection $\operatorname{pr}_2[\Gamma_\alpha \cdot (Z \times A)]$.

We shall be particularly interested in 1-cycles. Let C be a 1-cycle. If Y is a divisor on A, then we have the *transposition formula*

$$\deg(\alpha(C) \cdot Y) = \deg(C \cdot \tilde{\alpha}^{-1}(Y)). \tag{8}$$

The easy proof runs as follows.

$$\begin{aligned} \deg(\alpha(C) \cdot Y) &= \deg\{\operatorname{pr}_2[(\Gamma_\alpha \cdot (C \times A)) \cdot (A \times Y)]\} \\ &= \deg\{((C \times A) \cdot \Gamma_\alpha) \cdot (A \times Y)\}, \end{aligned}$$

because the degree of a 0-cycle is preserved under projection. All that remains to be done is to use associativity, and then unwind the above expression with respect to Y, just as we have done with respect to C.

We can transfer to the 1-cycles properties of divisors by transposition. For $\alpha, \beta \in H(A)$ we define

$$Z_C(\alpha, \beta) \equiv (\alpha + \beta)(C) - \alpha(C) - \beta(C), \qquad Z_C(\alpha) \equiv Z_C(\alpha, \delta),$$

* This section was added March 22, 1957.

these being elements of $N_1(A)$. We get trivially

(9) $$\deg[Z_C(\alpha,\beta)\cdot Y] = \deg[C\cdot D_Y(\alpha,\beta)].$$

This shows that $Z_C(\alpha,\beta)$ gives a bilinear map of $H(A)$ into $N_1(A)$, and D4 becomes $Z_C(\alpha,\alpha)\equiv 2\alpha(C)$. In addition, we obtain

(10) $$(m\alpha+n\beta)(C)\equiv m^2\alpha(C)+mnZ_C(\alpha,\beta)+n^2\beta(C)$$

(11) $$(\alpha+n\delta)(C)\equiv n^2C+nZ_C(\alpha)+\alpha(C).$$

In order to apply a numerical calculus dual to the intersection calculus of cycles used in Section 2, we must define the Pontrjagin product of cycles on A as follows. Let V, W be two subvarieties of A. By $V\oplus W$ we shall denote the set theoretic sum of V and W taken in A. It is the variety consisting of all points $v+w$ with $v\in V$ and $w\in W$. There is a rational map $F\colon V\times W\to V\oplus W$ which may or may not be of finite degree. By $d(V,W)$ we denote the degree of F if it is finite, and 0 otherwise. Similarly, we define $d(V_1,\cdots,V_m)$ for any finite number of subvarieties of A to be the degree of the rational map from their product to their set theoretic sum if it is finite, and 0 otherwise. We denote by $V*W$ the cycle $d(V,W)(V\oplus W)$, and one sees immediately that $V*W=\mathrm{pr}_3[S\cdot(V\times W\times A)]$, where S is the graph of the sum $s_2\colon A\times A\to A$. Note that $V*W=0$ if and only if the dimension of $V\oplus W$ is smaller than $\dim V+\dim W$. From the definitions, one also sees that the Pontrjagin product is associative, and that $V_1*V_1*\cdots*V_m=d(V_1,\cdots,V_m)(V_1\oplus V_2\oplus\cdots\oplus V_m)$. The product extends naturally to cycles by linearity, and if Z_1, Z_1 are two cycles, then

$$Z_1*Z_2=\mathrm{pr}_3[S\cdot(Z_1\times Z_2\times A)].$$

From the fact that the expression on the right is built up from the standard operations of intersection theory, we see that the Pontrjagin product defines a commutative ring structure on the graded module $\sum N_i(A)$.

Let $\alpha\in H(A)$. Then α induces an endomorphism of our ring, i.e., we have

(12) $$\alpha(V_1*V_2*\cdots*V_m)=\alpha(V_1)*\alpha(V_2)*\cdots*\alpha(V_m).$$

This is easily seen by applying the definitions. We are now in a position to use the same method as in Section 2 to get an expression for the characteristic polynomial $\nu(\alpha+n\delta)$, except that we use the Pontrjagin product instead of the intersection product. We are mostly interested in the trace. Raising both sides of (11) to the r-th power, using (12), we get

(13) $$\mathrm{tr}(\alpha)=r/d(C,\cdots,C)\cdot\deg[C^{*(r-1)}*Z_C(\alpha)],$$

provided we take for C a curve which generates A. Here, $C^{*(r-1)}$ means the

Pontrjagin product of C with itself $(r-1)$ times, and the degree is defined to be the coefficient of A appearing in the expression on the right. It is convenient to transform this expression into an intersection number. Whenever V and W have complementary dimesion, we have

$$d(V,W)=\deg(V\cdot W^{-})=\deg(V^{-}\cdot W), \tag{14}$$

denoting by V^{-} the transform of V by the map sending each point into its inverse. This is a restatement of an elementary result concerning algebraic groups (Weil [6], No. 13, Cor. 2 of Th. 4). If V is a divisor, then $V^{-}\equiv V$, say, by taking $\alpha=-\delta$ in the commutative diagram (4), and hence the expression for the trace becomes

$$\operatorname{tr}(\alpha)=r/d(C,\cdot\cdot\cdot,C)\cdot\deg(C^{*(r-1)}\cdot Z_C(\alpha)). \tag{15}$$

We have thus recovered all the numerical results contained in Weil's treatise on Abelian varieties. Consider the special case where $A=J$ is the Jacobian of a curve C. Then $C^{*(r-1)}=(g-1)!\Theta$, and $d(C,\cdot\cdot\cdot,C)=g!$. Using the transposition formula we get

$$\operatorname{tr}(\alpha)=\deg(D_\Theta(\alpha)\cdot C). \tag{16}$$

We remark that if we had tried to obtain this directly from the expression of the trace obtained by the ordinary intersection product, we would have needed the extra information that

$$\Theta^{(g-1)}\equiv(g-1)!C \text{ and } \deg(\Theta^{(g)})=g!.$$

Remarkably enough, there does not seem to be an easy proof available for this fact. Such a proof would require a closer analysis of the relations which exist between the ordinary and the Pontrjagin products of cycles.

Formula (16) allows us to recover the Lefschetz fixed point formula (and hence the Riemann hypothesis for curves), for we can now use the proof given by Weil ([6], No. 47) which is quite transparent. For the convenience of the reader, we reproduce this proof. If T is a correspondence on C (i.e., a 1-cycle on $C\times C$), we let τ be the associated endomorphism of J. The fixed point formula states that

$$\deg(T\cdot\Delta)=d(T)-\operatorname{tr}(\tau)+d'(T).$$

We let s_2 be the sum on $J\times J$, and consider the following diagram:

$$\begin{tikzcd}
C\times C \arrow[r, "f_2"] & J\times J \arrow[r, "(\tau,\delta)"] & J\times J \arrow[r, "s_2"] & J \\
C \arrow[u, "h_i"] \arrow[r, "f"'] & J \arrow[u, "H_i"'] & &
\end{tikzcd}$$

Here, f is the canonical mapping, f_2 is the product of f with itself, and h_i, H_i $(i=1,2,3)$ are described as follows: For $i=1$ we take the diagonal mapping. For the others, we may assume that we have a point P on C such that $f(P)=0$ is the origin on J. Then h_2 maps C on $P\times C$ and h_3 maps C on $C\times P$. Similarly, H_2 maps J on $0\times J$ and H_3 maps J on $J\times 0$. Then the square is commutative. Put $\lambda=(\tau,\delta)$. Then $f_2^{-1}\lambda^{-1}s_2^{-1}(-\Theta)$ is a correspondence T on $C\times C$ whose associated endomorphism is precisely τ. (Of course, in taking our inverse mappings, we first make a generic translation on Θ.) Furthermore, we have

$$s_2\lambda H_1=\tau+\delta,\qquad s_2\lambda H_2=\delta,\qquad s_2\lambda H_3=\tau.$$

From the commutativity, it is then obvious that

$$\deg[(\tau+\delta)^{-1}(-\Theta)\cdot C]=\deg(T\cdot\Delta),\qquad \deg[\tau^{-1}(-\Theta)\cdot C]=d(T),$$
$$\deg(-\Theta\cdot C)=d'(T).$$

This concludes the proof.

4. Positive endomorphisms. We shall say that an element α in $H_Q(A)$ is *symmetric* if $\alpha=\alpha'$. These elements form a subspace $S_Q(A)$ of $H_Q(A)$ over the rational numbers. We have a Q-linear map $D_X\colon S_Q(A)\to N_Q(A)$, defined by $\alpha\to D_X(\alpha)$. It is in fact an isomorphism, and we shall define its inverse $\Phi_X\colon N_Q(A)\to S_Q(A)$ as follows. If Y is a divisor representing a class in $N(A)$ then we put $\Phi_X(Y)=\frac{1}{2}\varphi_X{}^{-1}\varphi_Y$. The map $Y\to\Phi_X(Y)$ clearly induces a Q-linear map of $N_Q(A)$ into $H_Q(A)$. The commutativity relations (3) and (4) show that it is into $S_Q(A)$, i.e., that $\varphi_X{}^{-1}\varphi_Y$ is symmetric. From (7), we see that $D_X\Phi_X$ and $\Phi_X D_X$ are both equal to the identity, and hence are isomorphisms.

If Y is a divisor representing a class in $N(A)$, we shall write $\alpha\leftrightarrow Y$ to mean that $\alpha=\Phi_X(Y)$.

PROPOSITION 1. *Let α be a symmetric element of $H_Q(A)$, and suppose $\alpha\leftrightarrow Y$. Let λ be any element of $H_Q(A)$. Then $\lambda'\alpha\lambda\leftrightarrow\lambda^{-1}(Y)$. In particular, $\lambda'\lambda\leftrightarrow\lambda^{-1}(X)$.*

Proof. This is a reformulation of D10.

We shall say that an element of $H_Q(A)$ is *positive* (relative to the divisor X) if it is symmetric, and if there exists an integer $m>0$ such that the class of $D_X(m\alpha)$ in $N(A)$ contains a divisor $Y>0$. We then write $\alpha>0$.

PROPOSITION 2. *Let α be symmetric.*

a.) *If $\alpha \geqq 0$, and λ is any element of $H_{\mathbf{Q}}(A)$ then $\lambda'\alpha\lambda \geqq 0$.*

b.) *If $\lambda \in H_{\mathbf{Q}}(A)$ and $\lambda \neq 0$, then $\lambda'\lambda > 0$.*

c.) *If $\alpha > 0$, then* $\mathrm{tr}(\alpha) > 0$.

Proof. Our statements are immediate from Proposition 1 and the definitions.

As a corollary to Theorem 2, we shall see that if $\alpha > 0$ and $\lambda'\alpha \neq 0$, then actually $\lambda'\alpha\lambda > 0$.

We shall give below some equivalent conditions for an endomorphism to be positive. Referring to Albert [1] and Morikawa [5] we recall first an abstract theorem for the convenience of the reader.

THEOREM 2. *Let R be an algebra over the rationals $\mathbf{Q}$, with an involution $x \to x'$ satisfying $(xy)' = y'x'$ and $(x')' = x$, and a $\mathbf{Q}$-linear functional $\sigma: R \to \mathbf{Q}$ which satisfies $\sigma(xy) = \sigma(yx)$, and such that for $x \neq 0$ we have $\sigma(xx') > 0$. Then:*

1.) *R is semisimple.*

2.) *If $x = x' \neq 0$, then $\mathbf{Q}[x]$ is a direct sum of totally real fields.*

3.) *If $x = x' \neq 0$, then $\sigma(yxy) \geqq 0$ for all $y \in \mathbf{Q}[x]$ if and only if x is a sum of squares in $\mathbf{Q}[x]$.*

Proof of 1. We first prove that if $x = x' \neq 0$, then x cannot be nilpotent. If it were, then we would have $x^{2^m} = 0$ but $x^{2^{m-1}} \neq 0$, and hence $x^{2^m} = (x^{2^{m-1}})^2 = 0$. As $x^{2^{m-1}}$ is symmetric, this contradicts the strict positivity of σ. Now if $x \neq 0$ is an element of a nilpotent right ideal, then xx' is symmetric, is in the ideal, and hence is nilpotent, thereby contradicting again the positivity of σ.

Proof of 2. Consider $\mathbf{Q}[x]$ with $x = x' \neq 0$. It is a commutative subalgebra of R, and the involution and trace on R induce on it an involution and trace with similar properties. Being semisimple, it is a direct sum of fields. On each such field F we have again induced an involution and a trace. We may therefore assume that $R = F$. But any $\mathbf{Q}$-linear function on F is of type $\sigma(\xi) = S(\alpha\xi)$ for some α in F. Here S denotes the ordinary trace from F to $\mathbf{Q}$. We have by assumption $S(\alpha\xi^2) = \sigma(\xi^2) > 0$, if $\xi \neq 0$. If some conjugate of α is not real, then the corresponding conjugate of F is dense in the complex numbers, and we choose $\xi \in F$ such that $\alpha\xi^2$ is very large negative at this conjugate, and very close to 0 everywhere else. This gives a

contradiction, and α is totally positive. Similarly, one sees that R is totally real.

Proof of 3. We may again assume that $R=F$ is a totally real field. Then $\sigma(x\xi^2)>0$ for all $x\neq 0$ in F, and as we have seen above, this implies that x is totally positive. Hence it is a sum of squares. The converse is equally clear. This concludes the proof of our theorem.

COROLLARY 1. *Let R me as in the theorem, and $\xi\in R$ be such that $\xi=\xi'$, and $\sigma(\lambda\xi\lambda)\geqq 0$ for all $\lambda\in \boldsymbol{Q}[\xi]$. Then given $\beta\in R$ such that $\beta'\xi\beta\neq 0$, we have $\sigma(\beta'\xi\beta)>0$.*

Proof. We can write $\xi=\sum y_i^2$ with $y_i\in\boldsymbol{Q}[\xi]$. If we put $\mu_i=y_i\beta$, then at least one element $\mu_i'\mu_i$ is not 0, and

$$\sigma(\beta'\xi\beta)=\sum\sigma(\mu_i'\mu_i)>0.$$

COROLLARY 2. *Let R be as in the theorem, let $\alpha=\alpha'$ and assume that α is a sum of squares in $\boldsymbol{Q}[\alpha]$. If $\lambda\in R$ and if $\lambda'\alpha\neq 0$, then $\lambda'\alpha\lambda\neq 0$.*

Proof. Writing $\alpha=\sum\beta_i^2$ with $\beta_i\in\boldsymbol{Q}[\alpha]$, we must have $\lambda'\beta_i\neq 0$ for some i. Hence $0\neq(\lambda'\beta_i)(\lambda'\beta_i)'=\lambda'\beta_i^2\lambda$. Since $\sigma(\lambda'\beta_i^2\lambda)\geqq 0$ for each i, and for at least one i is >0, this shows that $\lambda'\alpha\lambda$ cannot be 0.

THEOREM 3. *Let $\alpha\in H_{\boldsymbol{Q}}(A)$ and assume $\alpha=\alpha'\neq 0$. Then the following conditions are equivalent:*

1.) *α is positive.*
2.) *All the characteristic roots of α are totally real and totally positive.*
3.) *α is a sum of squares in $\boldsymbol{Q}[\alpha]$.*

Proof. The equivalence between 2.) and 3.) is well known. If α is positive, and $\beta\in\boldsymbol{Q}[\alpha]$ then by D10 and the definition of the trace, we see that $\operatorname{tr}(\beta\alpha\beta)\geqq 0$. Hence α is a sum of squares by Theorem 2. This proves that the first condition implies the third. If we can write $\alpha=\sum\beta_i\beta_i'=\sum\beta_i^2$ with $\beta_i\in\boldsymbol{Q}[\alpha]$, then there is an integer $e>0$ and there are positive divisors Y_i such that $(e\beta_i)(e\beta_i)'=\varphi_X{}^{-1}\varphi_{Y_i}$ (Proposition 1). Putting $Y=\sum Y_i$, we see that $e^2\alpha=\varphi_X{}^{-1}\varphi_Y$, and hence that α is positive.

COROLLARY 1. *If α and β are two symmetric elements of $H_{\boldsymbol{Q}}(A)$ such that $\alpha>0$, $\beta>0$ and $\alpha\beta\neq 0$, then $\operatorname{tr}(\alpha\beta)>0$.*

Proof. We write $\alpha=\sum\lambda_i^2$ with $\lambda_i\in\boldsymbol{Q}[\alpha]$, and we have therefore $\operatorname{tr}(\alpha\beta)=\sum\operatorname{tr}(\lambda_i^2\beta)=\sum\operatorname{tr}(\lambda_i\beta\lambda_i)\geqq 0$. Actually, for some i, we have

$\lambda_i\beta \neq 0$, and hence by Corollary 2 of Theorem 2, $\lambda_i\beta\lambda_i \neq 0$. Hence the strict inequality holds, as desired.

COROLLARY 2. *Let $Y > 0$ be a divisor on A, and $Z^* > 0$ a divisor on $\hat{A}$. If $\alpha = \theta^{-1}\varphi_Z \cdot \varphi_Y$ and $\alpha \neq 0$, then* $\operatorname{tr}(\alpha) > 0$.

Proof. Let $\lambda = \varphi_X^{-1}\varphi_W$ with $W = \varphi_X^{-1}(Z^*)$ and let $\beta = \varphi_X^{-1}\varphi_Y$. We use the commutativity relations (3) and (4) to conclude that $\alpha = \lambda\beta$, and we can then apply Corollary 1.

Finally, note that if the abelian variety is defined over a finite field k with q elements, if X is rational over k, and if π is the Frobenius endomorphism, then from the relation $\pi\pi' = q\delta$, we can conclude from the above considerations without taking powers of π that the characteristic roots have absolute value $q^{\frac{1}{2}}$. Indeed, the algebra generated over $\boldsymbol{Q}$ by π and π' is commutative, and, in view of Theorem 2, is a direct sum of fields which are either totally real, or totally imaginary such that $x \to x'$ is the complex conjugation. If e_i is the idempotent of one of those fields, and if we put $\pi_i = \pi e_i$, then we see directly that the absolute value of π_i is $q^{\frac{1}{2}}$.

Appendix.

We shall now reproduce Weil's proof that if X is a divisor, $X \equiv 0$, then X is numerically equivalent to 0. The only property of abelian varieties that is used is the theorem of the square. To begin with, we have:

THEOREM. *Let $f\colon C \to A$ be a rational map of a complete non-singular curve into A, such that $f(C)$ generates A* (i.e., $A = f(C) + \cdots + f(C)$ *n times, where $n = \dim A$). Let $W = \sum_{1}^{n-1} f(C)$. Let $X \equiv 0$ be a divisor on A, and let*

$$f^{-1}(X) = \sum m_j(P_j).$$

(If necessary, make a generic translation on X so that $f^{-1}(X)$ is defined.) Let $M_1, \cdots, M_n$ be independent generic points of C over a common field of definition k for f, C, and A, and let

$$d = [k(M_1, \cdots, M_n) : k(\sum_{i=1}^{n} f(M_i))], \quad d_0 = [k(M_1, \cdots, M_{n-1}) : k(\sum_{i=1}^{n-1} f(M_i))].$$

Then $dX \sim nd_0 \sum m_j W_{f(P_j)}$.

Proof. Let $f_n\colon C \times \cdots \times C \to A \times \cdots \times A$ be the product of f with itself n times, and s_n the sum on A. Let $F = s_n f_n$. Then d is the degree

of F. A standard computation yields $F \circ F^{-1}(X) = dX$. On the other hand, using step 1 in Theorem 1, we get

$$F^{-1}(X) \sim \sum_i f_n^{-1} p_i^{-1}(X), \text{ which is } \sum_j m_j \sum_{i=1}^{n} (C \times \cdots \times P_j \times \cdots \times C).$$

We shall take F of this, and see that it gives the desired result. Let G be the graph of F, and let P be a generic point of C. Then by F-VII$_6$ Th. 12, we first take $G(P)$ on the product $C \times \cdots \times \hat{C} \times \cdots \times C \times A$ (where C is omitted in the i-th place), i. e., we take the projection on this variety of

$$G \cdot (C \times \cdots \times P \times \cdots \times C \times A).$$

This is a variety, whose set theoretic projection on A is $W_{f(P)}$. Taking now its projection on A in the sense of intersection theory, we obviously get $d_0 W_{f(P)}$. If we work with a special point P_j which is a specialization of P, then we use the compatibility of intersection and projection with specializations, together with the fact that $W_{f(P)}$ has the uniquely determined specialization $W_{f(P_j)}$, to conclude the proof.

Now by the theorem of the square, we get

$$nd_0 \sum m_j (W_{f(P_j)} - W) \sim W_u - W \equiv 0,$$

where $u = nd_0 \sum m_j f(P_j)$. Consequently, we get $0 \equiv dX \equiv nd_0 (\sum m_j) W$. If we can prove that $\sum m_j = 0$, this will show immediately that $dX \sim W_u - W$ and will prove the numerical equivalence of X to 0. We are therefore reduced to proving the following lemma.

LEMMA. *Let Y be a divisor, $Y > 0$. Then Y cannot be $\equiv 0$.*

Proof. If $Y \equiv 0$, then for t generic on A, we have $Y_t \sim Y$. This would yield a representation of A into the complete linear system of Y, and thus a representation of A into the projective linear group. This representation must be trivial, and hence $Y_t = Y$, which is an absurdity.

It should be noted that Morikawa's Lemma 7 [5] is an immediate consequence of the above result, which, in fact, shows that the divisor W is non-degenerate. Cf. also Weil's arguments concerning the projective embedding of abelian varieties [7].

COLUMBIA UNIVERSITY.

REFERENCES.

[1] A. Albert, "On involutorial algebras," *Proceedings of the National Academy of Sciences*, vol. 41 (1955), pp. 480-482.

[2] I. Barsotti, "Il teorema di dualita per le varieta abeliane ed altri risultati," *Rendiconti di Matematica e delle sue applicazioni*, vol. 13 (1954), pp. 1-17.

[3] W. L. Chow, "Abstract theory of the Picard and Albanese varieties," to appear.

[4] H. Hasse, "Über die Riemannsche Vermutung in Funktionenkörpern," *Comptes Rendus du Congres International des Mathématiciens*, Oslo, 1936, pp. 189-206.

[5] H. Morikawa, "On abelian varieties," *Nagoya Mathematical Journal*, vol. 6 (1953), pp. 151-170.

[6] A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann et Cie., Paris, 1948.

[7] ———, On the projective embedding of abelian varieties, in the volume in honor of S. Lefschetz, Princeton, 1957.

[8] ———, "On the theory of complex multiplication," *Proceedings of the International Symposium on Algebraic Number Theory*, Tokyo-Nikko. 1955. pp. 9-22.

SCHWARZ'S LEMMA AND A SINGULARITY OF BRIOT-BOUQUET.*

By AUREL WINTNER.

1. The following lemma (in which

$$(1)\qquad f(z,w)=\sum_{m+n>0} c_{mn}z^m w^n \equiv \sum_{i=1}^{\infty} f_i(z,w),\text{ where } f_i=\sum_{m+n=i},$$

need not be divisible by z) contains (if (1) is chosen to be divisible by z) the classical result on the initial-value problem

$$(2)\qquad w'=g(z,w),\qquad w(z)|_{z=0}=0,\qquad (w'=dw/dz),$$

where g ($\equiv f/z$) is a function regular at $(z,w)=(0,0)$.

LEMMA. *Let a function $f(z,w)$ of two complex variables be regular on the dicylinder*

$$(3)\qquad |z|<1,\qquad |w|<1,$$

and let

$$(4)\qquad |f(z,w)|\leqq 1 \text{ on } (3)$$

and

$$(5)\qquad f(0,0)=0$$

[*hence*

$$(4\,\text{bis})\qquad |f(z,w)|<1 \text{ on } (3)].$$

Then the (singular) initial-value problem

$$(6)\qquad zw'=f(z,w),\qquad w|_{z=0}=0$$

has a unique solution $w=w(z)$ which is regular on the circle

$$(7)\qquad |z|<1.$$

It will be clear from the proof how this lemma can be worded so as to apply when the single equation (6) is replaced by a system, that is, when the w and the f of (6) are vectors.

* Received June 16, 1957.

2. Since (1) holds on (3), it follows from (4) that $| c_{mn} | \leqq 1$ (Cauchy), where sign of equality holds only if $f(z, w)$ is $w^m z^n$ times a constant of absolute value 1. In particular

$$(8) \qquad | c_{01} | < 1$$

unless (6) reduces to

$$(8\,\text{bis}) \qquad zw' = cw, \qquad w\,|_{z=0} = 0, \qquad (|c| \neq 1),$$

and (8 bis) is trivial, since its only solution is $w(z) \equiv 0$. But (8) is certainly sufficient for

$$(9) \qquad c_{01} \neq 1, 2, \cdots,$$

the "eigenvalue" condition of Briot and Bouquet, who have shown that, under the proviso (9), there must exist for (6) a unique regular solution $w(z)$ on *some* circle $|z| <$ const., in which, however, the "sufficiently small" value of the const. remains unspecified* (correspondingly, neither (3) nor (4), but merely the absolute convergence of (1) on *some* neighborhood of $(z, w) = (0, 0)$ is needed in this result).

Accordingly, the point in the lemma is the specification of the radius of regularity for $w(z)$, that is, the assertion that, under the assumption (4) for (1), the entire circle (7), admitted in (3) for $f(z, w)$, follows for $w(z)$.

3. Actually, the interest of the lemma lies in a final nature of the (normalized) absolute constants which it supplies.

First, if (4) is relaxed to the assumption that

$$(4^*) \qquad |f(z, w)| < 1 + \epsilon \text{ on } (3), \qquad (\epsilon > 0),$$

where $\epsilon > 0$, while all the other assumptions of the lemma are satisfied, then, no matter how small the positive constant ϵ may be, (6) need not have a

---

* For three variants of the proof of Briot and Bouquet, see, respectively, L. Schlesinger, *Einführung in die Theorie der Differentialgleichungen* (1900), pp. 103-107; E. L. Ince, *Ordinary differential equations* (1926), pp. 295-296; L. Bieberbach, *Theorie der gewöhnlichen Differentialgleichungen* (1953), pp. 68-69. The circle $|z| <$const., which results in this manner as an assured domain of regularity for $w(z)$, is very unsatisfactory. In fact, the procedures are such as to involve not only the prinicple of majorants but, what is worse, an appeal to the *calcul des limites* as well as an application of the local existence theorem of implicit functions (for the majorant). For a discussion of these matters in the regular case, cf. A. Wintner, Acta Math., vol. 96 (1956), pp. 142-156, and Rend. Palermo, ser. 2, vol. 5 (1957), pp. 275-287. The nature of the "best absolute constants" in the general case of (9) remains undecided.

solution $w(z)$ which is regular on (7). As a matter of fact, (6) *need not have any solution $w(z)$ (regular at $z=0$) if* (4) *is replaced by* (4*). This is shown by the example $f(z,w)=\epsilon z+w$, which satisfies (4*) but reduces the first of the equations (6) to $dw/dz=\epsilon+w/z$, a linear differential equation for which every solution $w=w(z)$ becomes singular at $z=0$ if $\epsilon=\text{const.}\neq 0$.

Secondly, if all assumptions of the lemma are satisfied, then the radius $(=1)$ of the circle (7) is the best absolute constant. What is more, $w(z)$ can become singular on the boundary of (7). In order to see this, choose $f(z,w)$ to be independent of w, say $f=f(z)$, and put $g(z)=f(z)/z$. Then (4) and (5) will be satisfied if $g(z)$ is regular on (7) and $|g(z)|<1$ holds on (7). Since this is compatible with a function $g(z)$ having the circumference $|z|=1$ as a natural boundary, and since (6) now requires that $w(z)=\int g(z)dz$ (with $w(0)=0$), the assertion follows.

Remark. The *formal* source of all of this is the circumstance that $z\cdot(\ )'=zd(\ )/dz$ on the left of (6) as a ***homogeneous operator, of degree* 0, *in* z**. Let this operator be replaced by the ***identity operator***. Then (6) becomes replaced by

$$w=f(z,w),\qquad w\,|_{z=0}=0. \tag{6 bis}$$

And there results a correct statement *if* (6 bis) *is read, in place of* (6), *in the lemma of* § 1 (and if all the other assumptions, and the assertion, of the lemma are retained). This variant of the lemma, a theorem concerning implicit functions (rather than singular diffeerntial equations) is of a standard type. It can be proved, for instance, along the lines of Rouché's theorem, by appealing to general fixed point theorems (Poincaré-Brouwer).

Another proof for the case (6 bis) follows directly along the lines of the proof to be given for the case (6). But the resulting approach to (6 bis) is more straightforward (cf. § 11), since it does not involve, as (6) does, a Schwarzian lemma (cf. § 4). This contrast makes sufficiently clear the actual content of the lemma of § 1.

4. The proof of the italicized statement of § 1 will substantially depend on the following corollary of Schwarz's lemma (which explains the title of this paper):

Let $g(z)$ be a function which is regular for $|z|<1$, vanishes at $z=0$,

and satisfies the inequality $|g(z)| < 1$ *for* $|z| < 1$. *Let* $w = w(z)$, *where* $|z| < 1$, *denote the (unique, regular) solution of the initial-value problem*

$$(10) \qquad zw' = g(z), \qquad w|_{z=0} = 0.$$

Then $|w(z)| < 1$ *for* $|z| < 1$.

In fact, if $h(z) = g(z)/z$, then $|h(z)| < 1$ for $|z| < 1$. But (10) means that

$$w(z) = \int_0^z h(\zeta)\,d\zeta; \text{ hence } |w(z)| \leqq \int_0^{|z|} |d\zeta|,$$

and so $|w(z)| \geqq |z|$, where $|z| < 1$.*

5. This Schwarzian lemma will now be combined with the process of successive approximation, which will be set up as follows:

$$(11) \qquad zw_{k+1}'(z) = f(z, w_k(z)), \qquad w_{k+1}(0) = 0,$$

where $w_0(z)$ is any function which is regular on (7) and satisfies the case $k = 0$ of the following pair of conditions:

$$(12) \qquad |w_k(z)| < 1 \text{ on } (7), \text{ and } w_k(0) = 0$$

(for instance, $w_0(z) \equiv 0$).

Suppose that, for a fixed $k \geqq 0$, the function $w_k(z)$ has been defined on (7) so as to be regular and to satisfy (12). Then, since $f(z, w)$ is regular on (3) and satisfies (4) and (5), the function $g_k(z) = f(z, w_k(z))$ is regular on (7), satisfies $|g_k(z)| < 1$ on (7), and $g_k(0) = 0$. Hence, if (11) is identified with (10), it follows from the lemma of § 4 that $w_{k+1}(z)$ is regular on (7) and satisfies $|w_{k+1}(z)| < 1$ on (7). This completes the induction.

6. It will be shown in § 7 that the sequence

$$(13) \qquad w_1(z), \cdots, w_k(z), \cdots, \quad \text{where } w_k(0) = 0,$$

is convergent on a certain circle

$$(14) \qquad |z| < d, \qquad (d \leqq 1),$$

* The *best* estimate of $|w'(z)|$ for *fixed* z and *variable* g in (10) is supplied by a substantially deeper result of Dieudonné (depending on Pick's non-euclidean formulation of Schwarz's lemma; cf. p. 18 of Carathéodory's *Funktionentheorie*, vol. 2, 1950) which, however, does not lead to $|w(z)| < 1$ on $|z| < 1$ for *fixed* g.

for which the value of d will not be determined. But since the functions (13) are regular on (7) and satisfy (12), it will follow from the oldest theorem (Stieltjes) of the theory of normal families that the sequence (13), being convergent on (14), must be uniformly convergent on every closed subset of (7).

Let $w(z)$ be the limit function of (13) on (7). Then $w(z)$ is regular on (7) and is a solution of (6). This follows from the uniformity of the convergence if (11) is written in the form

$$(15) \qquad w_{k+1}(z) = \int_0^z f(\zeta, w_k(\zeta))/\zeta \, d\zeta, \qquad (|z| < 1).$$

In fact, it is clear from (4), (5) and (12) that, in view of Schwarz's lemma, the integrand of (15) is regular and (in k) uniformly bounded on (7).

7. The proof of the convergence of (13) on (14) (if d is small enough) proceeds as follows:

Let (1) be written in the form

$$(16) \qquad f(z, w) = c_{10}z + c_{01}w + h(z, w), \text{ where } h(z, w) = \sum_{i=2}^{\infty} f_i(z, w).$$

Then $h(z, w)$ is regular on (3) and contains only terms of second or higher order (in z and w together), which implies that $\partial h/\partial w \to 0$ as $(z, w) \to (0, 0)$. Hence it is clear that there belongs to every $\epsilon > 0$ a pair of positive numbers, say $d = d_\epsilon$ and $D = D_\epsilon$, which are less than 1 and have the property that the absolute value of the difference $h(z, w^*) - h(z, w^{**})$ will not exceed $\epsilon \mid w^* - w^{**} \mid$ whenever z, w^*, w^{**} are complex numbers within the respective circles $|z| < d$, $|w^*| < D$, $|w^{**}| < D$. On the other hand, it is seen from (12) and from Schwarz's lemma that, if $D = D_\epsilon$ is fixed and $d = d_\epsilon$ is chosen small enough, then $|w_k(z)| < D$ will hold on (14) for every k. Consequently,

$$(17) \qquad |h(z, w_k(z)) - h(z, w_{k-1}(z))| \leqq \epsilon \, |w_k(z) - w_{k-1}(z)| \text{ on } (14),$$

where ϵ and $d = d_\epsilon$ are independent of k.

According to (11), (16) and (17),

$$(18) \qquad |zw_{k+1}'(z) - zw_k'(z)| \leqq 0 + (|c_{01}| + \epsilon) |w_k(z) - w_{k-1}(z)| \text{ on } (14).$$

But if the trivial case (8 bis) is disregarded, then (8) holds and so, if the postitive number ϵ (which thus far was arbitrary) is chosen small enough, the sum $|c_{01}| + \epsilon$ will be less than 1. Consequently, from (18),

$$(19) \qquad |zu_{k+1}'(z)| \leqq \theta \, |u_k(z)| \text{ on } (14),$$

where $\theta =$ const. < 1 and

$$u_k(z) = w_k(z) - w_{k-1}(z). \tag{20}$$

Finally, it is clear from (12) and from Schwarz's lemma that, if d is chosen small enough, the functions (20) will be such as to satisfy $|u_k(z)| < 1$ on (14) (in fact, $d < \frac{1}{2}$ is sufficient to this end). In addition, $u_k(0) = 0$, since $w_k(0) = 0$. Hence, if Schwarz's lemma is applied to (19) in the same way as it was applied to (10) in the proof of the italicized assertion of § 4, it is seen, by induction, that (19) leads to

$$|u_k(z)| < \text{const.}\, \theta^k \text{ on } (14). \tag{21}$$

In fact, since the operator zd/dz remains invariant under the substitution $z \rightarrow Rz$, where R is a positive (or just non-vanishing) constant, it is clear that in contrast with Schwarz's own lemma, its "integral" corollary, that formulated in § 4, is independent of the radius of the z-circle (so that $|z| < 1$ can be replaced by any $|z| < d$).

8. Since the (positive) constant θ is less than 1, the convergence of the sequence (13) on the circle (14), chosen in § 7, is clear from (21) and (20). According to § 6, this proves that (6) has a solution $w(z)$ which is regular on the entire circle (7). Hence, in order to complete the proof of the lemma of § 1, all that remains to be ascertained is that (6) cannot have two distinct solutions (which are regular at $z = 0$).

The truth of this assertion of uniqueness is trivial in the case (8 bis). Hence it is sufficient to consider the case (8). But (8) implies (9) and, according to Briot and Bouquet, (9) alone is sufficient in order that the solution $w(z)$ of (6) be unique (in a neighborhood of $z = 0$).

The classical proof of this fact depends on a comparison of coefficients. Another proof (valid in the case (8) only) results by an adaptation of the "Lipschitz" uniqueness proof, customary in the real field. In fact, if $w = w(z)$ and $w = v(z)$ are regular solutions of (6) on (14), then it is clear from § 7 that, corresponding to (19) and (20),

$$|zu'(z)| \leqq \theta\, |u(z)|, \text{ where } u(z) = w(z) - v(z) \tag{22}$$

and $\theta < 1$, holds on (14), if d is small enough. But (22) leads to what results if $u_k(z)$ is replaced by $u(z) = w(z) - v(z)$ in (21), which means that $w(z) \equiv v(z)$ holds (on (14) and, therefore, on (7)).

9. The italicized assertion of § 1 can be completed by the following facts:

Under the assumption of the Lemma of § 1,

(i) *both*

$$|w(z)| < 1 \text{ and } |w'(z)| \leqq 1, \text{ where } |z| < 1, \tag{23}$$

hold for the solution of (6) (*and the sign of equality is excluded in* (23) *unless* (1) *is of the form* $f(z,w) = Cz$, *where* $|C| = 1$);

(ii) *if* c_{10} *and* c_{01} *are the coefficients of the linear terms in* (1), *then the solution* $w(z)$ *vanishes identically unless* $|c_{01}| < 1$; *while if*

$$c_{01} \neq 1 \text{ and } c_{10} \neq 0, \tag{24}$$

then

$$w'(0) = a \neq 0, \text{ where } a = c_{10}/(1 - c_{01}) \tag{25}$$

(*so that* $w(z)$ *is schlicht near* $z = 0$);

(iii) *if* (24) *is satisfied, then the inverse,* $z = z(w)$, *of* $w = w(z)$, *where* $w(0) = 0$, *is schlicht, and less than* 1 *in absolute value, on the circle* $|w| < |a|^2$, *where* $a = c_{10}/(1 - c_{01})$.

If (i) and the second part of (ii) are granted, then (iii) follows if a result of Landau, which he obtained in connection with his treatment of the problem of Bloch's constant, is used in the same way as I used it recently (vol. 78 (1956), pp. 552-553, of this Journal) in the *regular* case, (2), of (6). In fact, it is sufficient to combine (23), (24) and (25) with theorem (*) on p. 552, loc. cit., in order to obtain (iii) (the proof of (*), depending on Landau's result, is on p. 553, loc. cit.). Accordingly, only (i) and (ii) remain to be proved.

10. It is clear from the process of sucessive approximations which led to $w(z)$ that $|w(z)| < 1$ for $|z| < 1$; cf. (3)-(7). Hence it is clear from (4) that the function $\phi(z) = f(z, w(z))$ is regular, and does not exceed 1 in absolute value, on the circle $|z| < 1$. In addition, $\phi(0) = 0$ and $w'(z) = \phi(z)/z$, by (5) and (6). It follows therefore from Schwarz's lemma that $|w'(z)| \leqq 1$ if $|z| < 1$, where the sign of equality is excluded unless $w(z) = Cz$, where $|C| = 1$.

This proves (i). Since the first part of (ii), that concerning the identical vanishing of $w(z)$, is contained in the remark made in connection

with (8)-(8 bis), only the assertion of the second part of (ii) remains to be proved.

That assertion assumes (24) and claims (25). Hence it is sufficient to verify that, whether (24) is satisfied or not,

$$(1 - c_{01})a = c_{10}. \tag{26}$$

But if (1) and $w(z) = w(0) + w'(0)z + \cdots$, where $w(0) = 0$ and $w'(0) = a$, are inserted in (6), then it is seen that

$$z(a + \text{const.}\, z + \cdots) = c_{10}z + c_{01}(az + \cdots) + \cdots,$$

where the dots are terms which are of second or higher order in z. Hence (26) is obvious.

11. It is easy to see how the theorem mentioned in the Remark of § 3 can be proved by the method applied above. The assertion of that theorem is that the implicit equation $w = f(z, w)$ possesses a unique solution $w = w(z)$, satisfying $w(0) = 0$, which is regular (and less than 1 in absolute value) on the entire circle $|z| < 1$, if $f(z, w)$ is regular on the dicylinder (3) and satisfies both (4) and (5).†

† In the particular case in which $f(z, w)$ is independent of z (so that (6 bis) reduces to $w = zf(w)$), this fact has the following variant: *If $f(w)$ is regular, and $|f(w)/w|$ is not less than a positive constant K, on the circle $|w| < 1$, and if $f = 0$ and $df/dw = 0$ at $w = 0$ (hence $K \geqq 1$), then the solution $w = w(z)$ of Lagrange's equation $w = zf(w)$ is a regular and schlicht function not exceeding 1 on the circle $|z| < \Omega(1/K)$, where*

$$\Omega(M) = (1 - \sqrt{(1 - M^{-2})})^2 M^3 \qquad (0 < M \leqq 1,\ \Omega(1) = 1)$$

(*and $\Omega(1/K)$ is the best absolute constant for every fixed K*). In order to see this, it is sufficient to put $F(w) = w/f(w)$, then to interchange the parts played by the variables z and w, and finally to apply the following theorem of Landau (quoted, after the correction of a misprint in the third line of the wording of the theorem on p. 91, from Valiron's *Fonctions Analytiques* (Paris, 1954), pp. 90-93): If a function $F(z)$ is regular, and does not exceed M in absolute value, on the circle $|z| < 1$, and if $F(0) = 0$ and $F'(0) = 1$ (hence, $0 < M \leqq 1$), then the local inverse, $z = \phi(w)$, of $w = F(z)$ is regular, and less than 1 in absolute value, on the circle $|w| < \Omega(M)$, and $\Omega(M)$ is the best absolute constant for every fixed M.

Correspondingly, if the preceding device of replacing z, w, f, K by $w, z, F, M = 1/K$ is used in the *reverse direction*, it is easy to verify that a result of Hartman and myself (Rend. Palermo, ser. 2, vol. 3 (1954), pp. 287-291) can simply be interpreted so as to state the following: *If $w = F(z)$, where $F(0) = 0$, is a regular function satisfying $|F(z)| \geqq |z|$ for $|z| < 1$, then the circle $|z| < 1$ is the (schlicht) image of a* convex *w-domain contained in the circle $|w| < 1$* (and containing, of course, the point $w = 0$). The wording of this curious assertion becomes understandable only if it is noted that, as readily seen from Rouché's theorem, the whole of the circle $|w| < 1$ must be contained in the w-image of the circle $|z| < 1$ (an image which is *schlicht* by necessity), if $w = F(z)$, where $F(0) = 0$, is a regular function satisfying $|F(z)| \geqq |z|$ for $|z| < 1$.

First, (4) and (5) imply that $|f(z,w)| < 1$ on (3), and so it follows from (1) that (8) holds unless $f(z,w)$ is of the form $c_{01}w$ (where $|c_{01}| = 1$). But the latter case can be disregarded, since it leads to the trivial solution $w(z) \equiv 0$. On the other hand, (8) means, by (1), that the absolute value of the partial derivative $f_w(z,w)$ is less than 1 at the point $(z,w) = (0,0)$, and so the partial derivative $(w - f)_w = 1 - f_w$ does not vanish there. Consequently, there exists a solution $w(z)$ on *some* circle $|z| < \epsilon$. But on such a circle, $w(z)$ can be obtained by the method of successive approximations also. For, in view of (8), there is available for (1) a uniform Lipschitz constant $\theta < 1$ on a sufficiently small dicylinder about the origin. The replacement of $|z| < \epsilon$ by $|z| < 1$ now follows, as above, by having recourse to Stieltjes' theorem on normal families.

12. Under appropriate restrictions on the terms actually occurring in (1), Briot and Bouquet and their successors* have dealt with the (local)

* For references, cf. p. 38 and p. 40 of Painlevé's article II, 15 in the *Enc. des Sci. Math.* (1910). In view of the comments which follow above, it is necessary to correct a curious oversight which runs through the literature initiated by pp. 95-100 of Borel's celebrated paper on divergent series (*Ann. Ec. Norm.*, ser. 3, vol. 16, 1899). There Borel proved for the case $N < \infty$ (of any polynomial not containing linear terms), and surmised for the case $N \leqq \infty$ (of any power series not containing linear terms; an extension subsequently proved, along the lines of Borel's treatment of the polynomial case $N < \infty$, by Rémoundos (1908); cf. footnote 124) in Painlevé's article, p. 38), that, if the differential equation is

$$z^2w' = bw + \sum_{i=2}^{N} f_i(z,w), \qquad (2 \leqq N \leqq \infty), \tag{27 bis}$$

where $f_i(z,w)$ is, as in (1) and (27) above, a form of degree i, and b is a negative constant (so that $f_1(z,w)$ certainly does *not* vanish identically), then the situation is as follows: Not only can the coefficients a_k of the formal solution $w(z) = a_2z^2 + \cdots$ of (27 bis) be calculated uniquely (Briot-Bouquet), but the Borel associate,

$$W(z) = \sum_{k=2}^{\infty} a_k z^k/k!, \text{ of } w(z) = \sum_{k=2}^{\infty} a_k z^k$$

will have a non-vanishing radius of convergence (which means that $|a_k/k!|^{1/k} = O(1)$, i.e., $|a_k|^{1/k} = O(k)$; this cannot be improved to $|a_k|^{1/k} = O(1)$, since $w(z)$ itself need not have a convergence circle). But in both editions of his *Leçons sur les séries divergentes* (p. 117 of the first edition (1901), p. 150 of the second edition (1928)), Borel misquotes his result, by claiming it simply for

$$z^2w' = \sum_{k=2}^{N} f_k(z,w), \tag{27_0 bis}$$

rather than only for (27 bis), where $0 > b \neq 0$ (or, at least, $\operatorname{Re} b < 0$). Actually, even if the formal existence of the power series $w(z)$ is granted in the case (27_0 bis), the proof for the convergence of the associated power $W(z)$ (for small $|z| > 0$) breaks down completely, since $0 < -1/b < \infty$ (or, at least, $0 > \operatorname{Re}(-1/b) < \infty$) is essential

problem which results if the differential operator zd/dz of the (non-local) lemma of § 1 is replaced, not by the identity operator of § 11 (which is again of degree 0), but by the differential operator z^2d/dz (of a positive degree); so that (6) becomes replaced by

$$z^2w' = f(z,w), \qquad w\,|_{z=0} = 0, \qquad w'\,|_{z=0} = 0, \tag{27}$$

where, as before, $f(z,w)$ is a function regular in a neighborhood of the point $(0,0)$ and vanishing at $(0,0)$. Suppose that not only $f_0(z,w) \equiv f(0,0) = 0$ but also $f_1(z,w) \equiv 0$ holds in (1) (this seems to be, but actually is not, the case in the literature initiated by Borel; cf. the preceding footnote). Then, with the exception of one point, the proof of the lemma of § 1 on (6) can be repeated. But that point, though only of a local nature, happens to be fundamental enough to vitiate the final result.

The same holds if the case $f_1(z,w) \equiv 0$ of (1) and (27) is generalized from $j = 2$ to any integer $j > 1$, as follows:

$$\text{(28a)} \quad z^jw' = f(z,w), \qquad\qquad \text{(28b)} \quad f(z,w) = \sum_{i=j}^{\infty} f_i(z,w),$$

where $f_i(z,w)$ is a form of degree i, as in (1). If $j = 1$, then (28a)-(28b) reduces to the differential equation of (6), since (5) was assumed in (6). Correspondingly, suppose that a function (28b), belonging to a given $j > 1$, is regular on the dicylinder (3) and satisfies (4).

Since $f_i(z,w) \equiv 0$ in (28 bis) if $i < j$, it is easily realized that, after j applications of Schwarz's lemma, the italicized lemma of § 4 can be extended (from $j = 1$ to any j) so as to lead to the following result: Corresponding to (11)-(13), where $j = 1$, the $1 + j$ conditions

$$z^jDw_k(z) = f(z, w_{k-1}(z))\,; \qquad D^hw_k(0) = 0, \qquad 0 \leqq h < j, \tag{11_j}$$

where $w_0(z) \equiv 0$ and $D = d/dz$ (with $D^h = DD^{h-1}$ and $D^0v = v$), define for every k (> 0) a unique function $w_k(z)$ which is regular on (7) and satisfies the j inequalities

$$|\,D^hw_k(z)\,| < 1 \text{ on (7), where } 0 \leqq h < j \tag{12_j}$$

(in particular, (12) holds). Hence, the argument applied in the case $j = 1$ could be repeated without any change if the purely *local* aspect of the issue were in order, namely, if the sequence $w_1(z), w_2(z), \cdots$ of the successive

---

indeed in the majorization process on which the proof depends in the case (27 bis). Curiously enough, the error is repeated in the report of Painlevé (p. 38, loc. cit., is so explicit as to say that *b peut être nul*), who must have been misled both by Borel's and Rémoundos' mistaken formulations of what they had actually proved.

approximations, just secured on (7), were convergent on *some* circle $|z| < \epsilon$, as in § 7.

But precisely this classical (local) part of the issue leads to difficulties if the fixed j is greater than 1 in the initial value problem which, for a function $w(z)$ in a neighborhood of $z = 0$, is assigned by

$$(28c) \qquad D^h w(0) = 0, \qquad 0 \leqq h < j,$$

and (28a), with (28b). Apparently, the difficulties cannot be overcome without placing very specific restriction (to be supplied by a Newton polygon) on the set of the $j+1$ coefficients a_{mn} of the leading term,

$$(1_j) \qquad f_j(z, w) = \sum_{m+n=j} c_{mn} z^m w^n, \qquad (f_j \not\equiv 0),$$

of the double power series (28b). [Correspondingly, it is possible to allow in the power series (1) of (28a) a leading term $f_i(z, w)$ having a degree $i = i_0$ lower than the exponent j on the left of (28a), provided that still more specific restrictions are placed on the $i_0 + 1$ coefficients c_{mn} of that leading term.]

Appendix I.

If the function $g(z, w)$ occurring in (2), § 1, is now denoted by $f(z, w)$, then the classical result of the successive approximations, the result referred to at the beginning of § 1, is as follows:

(i) *If $f(z, w)$ is regular on the dicylinder*

$$(1) \qquad (|z| < 1, |w| < 1)$$

and if $f(z, w)$ is bounded,

$$(2) \qquad |f(z, w)| \leqq M \text{ on } (1),$$

then the solution $w = w(z)$ of the initial-value problem

$$(3) \qquad dw/dz = f(z, w), \qquad w|_{z=0} = 0$$

exists, as a regular function satisfying

$$(4) \qquad |w(z)| < 1,$$

on the circle

$$(5) \qquad |z| < \min(1, M^{-1})$$

(*at least*). With regard to the last (parenthetical) remark, it is known that

the radius of the circle (5) is the best *absolute* constant for every fixed value of the positive constant M occurring in (2); cf. my note in vol. 57 (1935), pp. 539-540, of this Journal.

Whereas the assumption (2) of (i) represent an *upper* limitation, (i) has a curious counterpart, (ii) below, in which only a *lower* limitation, $|f(z,w)| \geqq K = \text{const.} > 0$, is assumed. But it will be clear from the proof that K cannot be allowed to be less than 1; so that, in view of the comments made in the first part of § 3, the resulting dual of (i) lies along the lines of the Lemma (§ 1), rather than of (i) itself. The dual of (i) in question, which I considered in a rough form (and, in addition, in terms of a normalization which disguises the true situation) on pp. 551-553 of vol. 78 (1956) of this Journal, is as follows:

(ii) *Let $f(z,w)$ be regular on* (1) *and, on* (1), *let $|f(z,w)|$ be bounded from below by a constant which is not less than* 1 *(i.e., let*

$$K \geqq 1, \text{ and } |f(z,w)| \geqq K \text{ on } (1), \tag{6}$$

while (2) *need not hold for any $M < \infty$). Then the solution $w = w(z)$ of* (3) *exists, as a regular function satisfying* (4), *on the circle*

$$|z| < \phi(\theta), \text{ where } \theta = K/|f(0,0)| \tag{7}$$

[hence, $0 < \theta \leqq 1$, *by* (6)], *if $\phi = \phi(\theta)$ denotes the (positive, increasing) function*

$$\phi(\theta) = 1 - (1 - \theta^{-2}) \log(1 - \theta^2), \qquad (0 < \theta \leqq 1), \tag{8}$$

where $\phi(+0) = 0$, $\phi(1) = 1$.

Remark. It will be clear from the proof that *either the regular function element $w = w(z)$, given on the circle* (7), *or a direct analytic prolongation of this function element must attain, at some $z = z(w)$, every value w contained in the circle $|w| < 1$.* But this, together with the fact that (3) and (6) imply the non-vanishing of $dw(z)/dz$ (hence the *unramified* character of the inverse function) on (7), does not of course mean that $w(z)$ is *schlicht* on the circle (7).

The proof of (ii) will follow by an appropriate combination of two known facts, those listed under (I) and (II) below. The application of these two facts will be made possible by writing (3) in the form

$$dz/dw = 1/f(z,w), \qquad z|_{w=0} = 0, \tag{9}$$

i.e., by first interchanging the parts played by z and w.

(I) The classical result (the result which supplies the radius of (5) if $a = 1$ and $b = 1$) states that if $f(z, w)$ is regular, and does not exceed M in absolute value, on a dicylinder $(|z| < a, |w| < b)$, then the solution $w = w(z)$ of (3) is regular, and satisfies the inequality $|w(z)| < b$, on the circle $|z| < \min(a, b/M)$.

(II) A theorem of Landau (his Satz X on p. 473 of his paper in the Sitzber. Preuss. Akad. Wiss., 1926) states that if a function $w = w(z)$ is regular, and has a derivative $w' = dw/dz$ satisfying the inequality $|w'(z)| \leqq S/R$, on the circle $|z| < R$, where R and S are given positive numbers, and if $w(0) = 0$ and $w'(0) \neq 0$, then the (local) inverse function, $z = z(w)$, of $w = w(z)$ (i.e., the function element $z(w)$ assigned, near $w = 0$, by $w(0) = 0$ or $z(0) = 0$) is regular, and less than R in absolute value, on the circle $|w| < S\phi(\theta)$, where θ and $\phi(\theta)$ are defined by $\theta = R\,|w'(0)|/S$ and (8) respectively (clearly, the assumption $0 < \theta \leqq 1$ of (8) is satisfied, and $\theta = 1$ holds only in the trivial case $f(z) = \text{const.}\, z$). Landau (loc. cit.) has also shown that the radius of his w-circle is the best absolute constant for any given triple of positive numbers $R, S, |w'(0)|$.

In order to prove (ii), suppose that $f(z, w)$ is regular on (1) and that there exists a constant K satisfying (6). Then, if z and w are interchanged, (3) becomes (9), and (I) is applicable when a, b, M and f are chosen to be 1, 1, K^{-1} and $1/f(z, w)$ respectively. Thus the radius of the w-circle supplied by (II) becomes $\min(1, K)$, which is 1, since $K \geqq 1$, by (6).

Accordingly, the solution $z = z(w)$ of (9) is regular, and satisfies the inequality $|z(w)| < 1$, on the circle $|w| < 1$. In addition, since $|1/f(z, w)| \leqq K^{-1}$ on (1), it follows from (9) that the absolute value of the derivative $dz(w)/dw$ does not exceed K^{-1} on the circle $|w| < 1$.

Consequently, if (II) is applied so as to interchange z and w, then the assumptions of (II) are satisfied when R, S and $|w'(0)|$ are chosen to be K, 1 and T respectively, where T denotes the value of $|dz(w)/dw|$ at $w = 0$. But (9) shows that $T = |f(0, 0)|^{-1}$, where $f(0, 0) \neq 0$, by (6). It follows therefore from (II) that the inverse function of $z = z(w)$, which is now the function $w = w(z)$, is regular, and satisfies the inequality $|w(z)| < 1$, on the circle (7). This proves (ii).

The question raised by the Remark, following (ii), can be answered if (II) is replaced by another theorem of Landau, which can be formulated as follows (cf., e.g., p. 95 of Valiron's *Fonctions Analytiques*, 1954):

(III) If $w(z)$ is regular, and satisfies the inequality $|w(z)| \leqq S$, on the circle $|z| < R$, and if $w(0) = 0$ and $w'(0) \neq 0$ (where $w' = dw/dz$),

then $w(z)$ is *schlicht* on the circle $|z| < R\psi(\theta)$, where $\theta = R\,|w'(0)|/S$ (hence, $0 < \theta \leqq 1$), if $\psi = \psi(\theta)$ denotes the (positive, increasing) function

$$(10) \qquad \psi(\theta) = [1 - (1 - \theta^2)^{\frac{1}{2}}]/\theta \qquad (0 < \theta \leqq 1)$$

(so that $\psi(+0) = 0$, $\psi(1) = 1$). Landau also proved that the radius of his z-circle is the best absolute constant for any given triple of positive numbers R, S, $|w'(0)|$.

(ii bis) *Under the assumption of* (ii), *there exists a positive* $\lambda = \lambda(\theta)$, *depending only on the ratio* $\theta = K/|f(0,0)|$ *and having the property that the solution* $w = w(z)$ *of* (3) *is schlicht on the circle* $|z| < \lambda(\theta)$.

In fact, it is clear from (ii) and (III) that a $\lambda = \lambda(\theta)$ satisfying the requirements of (ii bis) can be obtained by composing the two positive functions (8), (10). No such composition is needed in what corresponds to (ii bis) when (ii) is replaced by the classical result (i):

(i bis) *If* $f(z, w)$ *is regular on* (1) *and satisfies* (2), *then the solution* $w = w(z)$ *of* (3) *fails to be schlicht on any circle* $|z| < \epsilon$ *if* $f(0,0) = 0$; *while if* $f(0,0) \neq 0$, *and if* $\psi(\theta)$ *is defined by* (10), *then* $w(z)$ *is regular and schlicht on the circle* $|z| < \psi(f(0,0)|)$ *or on the circle* $|z| < \psi(|f(0,0)|/M)/M$ *according as* $M \geqq 1$ *or* $M \leqq 1$.

In fact, $w'(0) = f(0,0)$, by (3). Hence the assertion of (i bis) is obvious for the case $f(0,0) = 0$. In the remaining case, it is seen from (i) that (III) is applicable with $S = 1$, $|w'(0)| = |f(0,0)| > 0$, and $R = 1$ or $R = M^{-1}$ according as $M \geqq 1$ or $M \leqq 1$. It is readily verified from (10) that, in both subcases of the case $f(0,0) \neq 0$, the z-circle supplied by (i bis) is contained in (and, except in the trivial case $|f(0,0)| = M$, where $f(z, w) = \text{const.}$, is *smaller* than) the z-circle, (5), of (i) itself.

* *

*

Let finally be mentioned the following theorem (ii_0) which, on the one hand, represents the limiting case of (ii) and, on the other hand, can be interpreted as a refined form of (the local part of) a classical result (Briot-Bouquet, Fuchs, Poincaré) on the exceptional standing of Riccati's equation:

(ii_0) *If the coefficients of a quadratic polynomial*

$$(11) \qquad f(z, w) = \alpha(z)w^2 + \beta(z)w + \gamma(z)$$

are regular and bounded on a circle $|z| < a$, *and if* b, L *is a pair of positive*

constants having the property that the absolute value of the quadratic polynomial $\alpha(z)+\beta(z)w+\gamma(z)w^2$ *is less than* L *on the dicylinder* $(|z|<a, |w|<b)$, *then, unless* $\alpha(z)$ *vanishes identically, the (generalized Riccati) differential equation* $w'=f(z,w)$ *possesses on the circle*

$$(12) \qquad |z|<\min(a,(bL)^{-1})$$

a unique solution $w=w(z)$ *which is regular at every point* $z\neq 0$ *of the circle* (12) *and satisfies the "initial condition"* $w(0)=\infty$, *the function* $w(z)$ *having a pole at* $z=0$; *in addition,* $|w(z)|>b$ *on* (12).

Note that $w'=f(z,w)$ is a Riccati equation of standard type, reducible by the substitution $w=v'/v$ to the linear differential equation $w''+p(z)v'+q(z)v=0$ (where $p=-\beta$, $q=-\gamma$), only if $\alpha(z)$ is identically 1; and that, even without regard to the explicit value of the radius* of the circle (12), division by $\alpha(z)$ introduces a singularity (of the linear differential equation of second order) at $z=0$ if $\alpha(0)=0$, whereas the vanishing of $\alpha(0)$ is allowed in (ii_0), the only restriction being the not *identical* vanishing of $\alpha(z)$, i.e., the exclusion of the linear case, $w'=\beta(z)w+\gamma(z)$, of $w'=f(z,w)$ itself.

In order to prove (ii_0), put $u=1/w$, $F(z,u)=-u^2f(z,1/u)$, and $N=b^2L$. Then (11) and the definitions of a, b, L show that $F(z,u)$ is regular, and less than N in absolute value, on the dicylinder $(|z|<b, |u|<b)$. Hence, $u'=F(z,u)$ has on the circle $|z|<\min(a,b/N)$ a unique (regular) solution $u=u(z)$ satisfying $u(0)=0$, and $|u(z)|<b$ holds on this circle. Since the latter is precisely (12), the assertions of (ii_0) follow from $w(z)=1/u(z)$. The exclusion of the identical vanishing of $\alpha(z)$ is needed in order to prevent that $w(z)$ becomes ∞ identically.

---

* For the case in which $\alpha(z)$ and $\beta(z)$ are identical with 1 and 0 respectively (so that $w'=f(z,w)$ reduces to $w'=\gamma(z)+w^2$), a radius sharper than that of (12) was obtained by Dieudonné (Bull. des Scien. Math., vol. 55 (1931), part 2, pp. 99-104), whose result is of a final nature in this case. His method, based on an adaptation of Sturm's comparison theorem to the complex field, contains *in nuce* what, in my papers referred to in the footnote to § 2 above, I called the "principle of subordination," and which goes back to a note of Nakano (Proc. Imp. Acad. Japan, vol. 8 (1932), pp. 29-31), a note of a somewhat later date than Dieudonné's paper dealing with $w'=\gamma(z)+w^2$. For an extension of Dieudonné's result to other Riccati equations (and for systems of such equations), cf. M. Müller, Math. Ztschr., vol. 41 (1936), pp. 174-175. Dieudonné's Sturmian inequality and the final nature of his absolute constant were rediscovered by Z. Nehari (Bull. Amer. Math. Soc., vol. 55 (1949), p. 549).

Appendix II.

The theorem of Briot and Bouquet, referred to in § 2, states that the differential equation

$$(1) \qquad zw' = az + \beta w + \phi(z,w), \text{ where } \phi(z,w) = \sum_{m+n\geqq 2} a_{mn} z^m w^n,$$

possesses on *some* circle about $z = 0$ a unique solution

$$(2) \qquad w(z) = \sum_{k=1}^{\infty} c_k z^k,$$

if the power series $\phi(z,w)$ converges on a neighborhood of $(z,w) = (0,0)$ and a, β are two constants the second of which is not a positive integer. But no reasonable estimate is supplied for the radius of the circle (about $z = 0$) on which (2) is convergent, the methods of proof being those referred to in the footnote to § 2.

The purpose of the first part of this appendix is to fill in somewhat this gap, by obtaining (*via* § 11) an estimate which is explicit enough and, at the same time, is free of one of the weak points criticized in that footnote, *viz.*, of the step which involves the use of Cauchy's coefficient estimates (the "calcul des limites"). Still, the result to be obtained cannot possibly be of a final nature; in fact, two processess of majorization remain to be dispensed with.

In the latter part of this appendix, it will be shown that one at least of these two, substantially weakening, processes of majorization *can* be dispensed with (*via* § 1, rather than, as before, *via* § 11); so that just one of the three aspects criticized in the footnote to § 2 will ultimately remain. For it will turn out that, owing to the lemma of § 1, the majorization of the differential equation (1) by an "implicit equation" of the form $w = f(z,w)$, a majorization which since Briot and Bouquet is an essential point in all treatments of (1) (cf. the references in the footnote to § 2), can be avoided entirely.

The only remaining weak point will therefore be the majorization of (1) by a case of (1), with $\beta = 0$ but $a \geqq 0$ and $a_{mn} \geqq 0$ (the latter constants β, a, a_{mn} are not, of course, the same as in (1); the new a_{mn} is the absolute value of the old a_{mn}). But even this single process of majorization must prevent a result which is as sharp as possible (except as a result of majorization; cf. the first of my papers referred to in § 2). Correspondingly, what will be involved is only that (compartively straightforward) particular case of the lemma of § 1 in which the coefficients of the double power series $f(z,w)$ are $\geqq 0$.

If $h(z,w)$ is any power series, let $h^*(z,w)$ denote its *best majorant*, *i.e.*, put

$$h^*(z,w)=\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}|b_{mn}|z^mw^n \text{ if } h(z,w)=\sum_{m=0}^{\infty}\sum_{n=0}^{\infty}b_{mn}z^mw^n. \tag{3}$$

Thus $h^*(z,w)$ is convergent on a dicylinder

$$|z|<a, \qquad |w|<b \tag{4}$$

if $h(z,w)$ is, but the function $h^*(z,w)$ need not be bounded on (4) if the function $h(z,w)$ is. Suppose however that, if $\phi(z,w)$ is the power series occurring in (1), the radii of the dicylinder (4) are chosen so small that not only $\phi(z,w)$ but also $\phi^*(z,w)$ will be bounded on (4). Next, in terms of the second of the constants occurring in (1), a constant β which can be complex but is, by assumption, not a positive integer, define a positive number $\gamma=\gamma(\beta)$ by placing

$$\gamma=\min_{2\leqq n<\infty}|n-\beta|. \tag{5}$$

Finally, since 1 is a positive integer, hence $|\alpha/(1-\beta)|$, where α is the first of the constants occurring in (1), is a non-negative value distinct from ∞, it is possible to choose the radii of the dicylinder (4) so small that the inequality

$$|\alpha/(1-\beta)|a^2+\phi^*(a,b)a/\gamma\leqq b \tag{6}$$

becomes satisfied (in fact, since α, β and $\gamma=\gamma(\beta)>0$ are fixed, and since $\phi(z,w)$, hence $\phi^*(z,w)$, vanishes at $(0,0)$ in the second (collective) order (of z,w), at least, the inequality (6) will be satisfied by a sufficiently small $a>0$ even if $b=a$). The explicit result, to be proved, can now be formulated as follows:

If β is not a positive integer, γ is defined by (5), *and $a>0$ is chosen so small that* (6) *holds for some $b=b_a>0$, then* (1) *possesses a* (*unique*) *regular solution $w(z)$, with $w(0)=0$, on a circle $|z|<$ const. the radius of which is not less than a.*

First, if (2) is substituted into (1), comparison of like powers of z supplies for $k>1$ the recursion formula

$$(k-\beta)c_k=\Phi_k(c_1,\cdots,c_{k-1}), \qquad c_1=\alpha/(1-\beta), \tag{7}$$

where Φ_k is a polynomial (in $k-1$ variables), with coefficients which are polynomials in the coefficients a_{mn} of $\phi(z,w)$. Let $\Psi_k(c_1,\cdots,c_{k-1})$ denote the polynomial (with real, non-negative coefficients) which results if every a_{mn} is replaced by $|a_{mn}|$ in $\Phi_k(c_1,\cdots,c_{k-1})$. Then it is easily realized

from the definitions, (3) and (5), of the symbol * and of the number γ that the sequence of the absolute values $|c_1|, |c_2|, \cdots$ of the numbers $c_1, c_2, \cdots$ defined by (7) is majorized by the (real, non-negative) sequence $c_1, c_2, \cdots$ defined by

$$(8) \qquad \gamma c_k = \Psi_k(c_1, \cdots, c_{k-1}), \qquad c_1 = |a/(1-\beta)|,$$

where $k > 1$. On the other hand, it is clear from the definition of Ψ_k that substitution of (2) into

$$(9) \qquad \gamma w = \lambda z + \phi^*(z, w), \text{ where } \lambda = \gamma\,|a/(1-\beta)|,$$

leads to the first or to the second of the relations (8) according as $k > 1$ or $k = 1$. Hence, in order to prove that (1) possesses a solution $w = w(z)$, satisfying $w(0) = 0$, which is regular on a given circle $|z| < a$, it is sufficient to prove that (9) possesses such a solution on that circle.

Next, if $f(z, w)$ is regular, and $|f(z, w)|$ is less than a constant M, on a dicylinder (4), and if $f(0, 0) = 0$, then the equation $w = f(z, w)$ has on the circle $|z| < a$ a (unique) regular solution $w = w(z)$ satisfying $w(0) = 0$, provided that the inequality $M \leqq b/a$ is satisfied by a, b, M. For if all three constants a, b, M are normalized to be 1, then the assertion reduces to that of § 11. But if z, w and $w = f(z, w)$ are replaced by pz, qw and $rw = rf(z, w)$ respectively, where p, q, r are positive constants, then, by choosing the latter so as to render 1 the resulting values of a, b, M, the assertion follows.

Finally, let $w = f(z, w)$ be identified with what results if (9) is written in the form

$$(10) \qquad w = |a/(1-\beta)|\,z + \phi^*(z, w)/\gamma.$$

Then it is clear that $|f(z, w)| < M$ holds on (4) if M denotes the value which the sum occurring on the right of (10) attains at $(z, w) = (a, b)$. But this choice of M reduces the inequality $M \leqq b/a$ to the inequality (6). Thus § 11, when applied to the majorant (10) of (1), supplies precisely that explicit form of the Briot-Bouquet theorem which was italicized after (6).

Unfortunately, what was used here from § 11 is substantially more on the surface than § 11 itself, since all coefficients of the double power series $f(z, w)$ are non-negative in the case (10) of $w = f(z, w)$. Without this circumstance, produced by the process of majorization, a result sharper than (6) would follow from § 11.

* *

*

There is however an additional weak point in the majorization of (1) by (10). This point is the circumstance that the replacement of (7) by

(8), where γ is independent of k, implies the sacrifice of all the convergence-producing effects of the big factor $(k-\beta) \sim k \to \infty$ on the left of (7). But it turns out that this drastic step,† which goes back to Briot-Bouquet, can be avoided entirely.

Instead of the positive constant $\gamma = \gamma(\beta)$ defined by (5), introduce the positive constant $\mu = \mu(\beta)$ defined by

$$(11) \qquad \mu = \max_{2 \leq n < \infty} |n - \beta|/n;$$

so that $\mu > 0$, in contrast with $\gamma > 0$, does not fail to involve the fact that $(k-\beta)$ is large for large k. Nevertheless, the situation is as follows:

The statement italicized after (6) *remains true if the factor* $1/\gamma$ *of the second term in* (6) *is replaced by the factor* $1/\mu$ *defined by*

$$\mu = \max_{2 \leq n < \infty} |1 - \beta/n|$$

(*cf.* (5) *and* (11)).

In fact, it is clear from (11) and from the definition of Ψ_k that, instead of (8),

$$(8\,\text{bis}) \qquad \mu k c_k = \Psi_k(c_1, \cdots, c_{k-1}), \qquad c_1 = |a/(1-\beta)|$$

can be used as a majorant system of (7). But it is also clear that this majorant system belongs to the solution (2) of the *differential* equation

$$(9\,\text{bis}) \qquad \mu z w' = \lambda z + \phi^*(z, w), \text{ where } \lambda = \gamma\,|a/(1-\beta)|,$$

in the same way as (7) belongs to the solution (2) of the differential equation (1). Consequently, division by the constant $\mu > 0$ shows that if the differential equation

$$(10\,\text{bis}) \quad zw' = f(z, w), \text{ where } f(z, w) = |a/(1-\beta)|\,z + \phi^*(z, w)/\mu,$$

possesses a solution $w = w(z)$, satisfying $w(0) = 0$, which is regular on a given circle $|z| < a$, then such a solution $w(z)$ will exist, on the same circle, for (1) also. Consequently, the last italicized statement follows if § 1 is applied to (10 bis) in the same way as § 11 was applied to (10).

THE JOHNS HOPKINS UNIVERSITY.

† The possible effect of this step is well illustrated by the following example: If the recursion formula is $kc_k = c_{k-1}$, where $c_0 = 1$, then $w(z) = c_0 + c_1 z + \cdots$ is the solution $w(z) = \exp z$ of $w' = w$, whereas if the factor k is omitted on the left, then, since the recursion formula becomes $c_k = c_{k-1}$, there results the solution $w(z) = 1/(1-z)$ of $w = zw$. But whereas $\exp z$ is an entire function, $1/(1-z)$ is not.

REMARKS TO TWO PREVIOUS PAPERS

(vol. 69, 1947, pp. 87-98 and vol. 71, 1949, pp. 587-594).*

By Aurel Wintner.

Let $f(t)$ be a continuous function on the (for instance, open) half-line $(0,\infty)$, and consider the three differential equations

$$(1)\quad x''-f(t)x=0,\qquad (2)\quad y'=y^2-f(t),\qquad (3)\quad (\log x)'=-y,$$

the second of which is equivalent to the first by virtue of the third if $x(t)\neq 0$ (Riccati). A classical result of A. Kneser states that if $f(t)\geqq 0$, then (1) has a solution $x(t)$ which is positive and non-decreasing on $(0,\infty)$ (so that

$$(4)\qquad x(t)>0 \text{ and } x'(t)\leqq 0, \text{ hence } x''(t)\geqq 0,$$

since $x''=fx$, $f\geqq 0$), and this solution $x(t)$ of (1) is unique up to a positive constant factor. If appropriate additional conditions are placed on $f(t)\geqq 0$, then more than (4) can be said about Kneser's solution $x(t)$. This is exemplified by the sequence of successive conditions which, in the first of my papers quoted in the title of this note, led to the following result: If $f(t)$ is totally monotone (in the sense of the Hausdorff-Bernstein theorem), then the same is true of $x(t)$. The following remarks consider similar but different implications which refer to Riccati's $y(t)$ in (3), rather than to $x(t)$ itself, as follows:

(i) If $f(t)\geqq 0$ on $(0,\infty)$, then (2) possesses one and only one solution $y(t)$ which exists and satisfies $y(t)\geqq 0$ on the whole of $(0,\infty)$.

(ii) If $f(t)\geqq 0$ is non-increasing and differentiable, i.e., $f'(t)\leqq 0$, then also $y'(t)\leqq 0$ holds.

(iii) In addition, $y''(t)\geqq 0$, if $f(t)\geqq 0$ and $f'(t)\leqq 0$ are subject to

$$(5)\qquad 16f^3(t)\leqq 27f'^2(t).$$

(iv) If $f(t)\geqq 0$ is convex (from below),† so that $f''(t)\geqq 0$, then, whether (5) is satisfied or not, the assertions, $y'(t)\leqq 0$ and $y''(t)\geqq 0$, of (ii) and (iii) imply the assumption, $f'(t)\leqq 0$, of (ii).

* Received July 22, 1957.

† The derivatives f', f'' (and y'') occurring in the wording of (iv) are meant in the sense customary in the theory of measurable convex functions: f' as a unilateral derivative, which is absolutely continuous, and f'' as the derivative of f' almost everywhere.

Note that the assertions of (i), (ii), (iii) on $y(t)$ and its derivatives claim for (2) what, *without* the additional assumptions placed on $f(t) \geqq 0$ in (ii) and (iii), the inequalities (4) ensure for (1) by virtue of $f(t) \geqq 0$ alone. In fact, (i), (ii), (iii) can be summarized by saying that

$$f(t) \geqq 0, \quad f'(t) \leqq 0 \tag{6}$$

and (5) together imply that

$$y(t) > 0, \quad y'(t) \leqq 0, \quad y''(t) \geqq 0 \tag{7}$$

on $(0, \infty)$. On the other hand, neither the necessity nor the sufficiency of

$$f(t) \geqq 0, \quad f'(t) \leqq 0, \quad f''(t) \geqq 0 \tag{8}$$

for (7) follows from (iv).

It is easy to see that (8) cannot replace (6) and (5) for (7) (substantially more than this negation results from the example to be constructed at the end of this paper). On the other hand, it is not clear that (5) cannot be improved by diminishing the value of the absolute constant 27/4.

Proof of (i). It is seen from (3) that (i) is just a restatement of Kneser's theorem.

Proof of (ii). Draw in the half $t > 0$ of the (t, y)-plane the curves C_1: $y = y^*(t)$ and C_2: $y = -y^*(t)$, where $y^* = f^{\frac{1}{2}} \geqq 0$, and denote by P, Q, R the sets of those points of that half-plane which are situated, respectively, above C_1, between C_1 and C_2 (with the inclusion of the boundary $C_1 + C_2$), and below C_2. Then the solution curve C: $y = y(t)$, being, by (i), in the half-plane $y \leqq 0$, cannot have any point in P. If C had a point in R, then the method of the "curves of zero velocity" (cf. my note in the Quart. Journ. of Math. (Oxford), vol. 18 (1947), pp. 65-71) would lead to a situation which is contradicted by (2), since the "curves of zero velocity" are the present C_1 and C_2, and since, in view of the hypothesis of (ii), the (common) absolute value of the ordinates of C_1 and C_2 is a non-increasing function of t. Consequently, C stays in Q. In view of (2), this means that $y'(t) \leqq 0$, as claimed by (ii).

Proof of (iii). If (2) is differentiated and y' is substituted from (2) into the result, it follows that $y'' = 2\phi(y)$, where $\phi(y)$ denotes the case $a = f(t) \geqq 0$, $b = -\frac{1}{2}f'(t) \geqq 0$ of the cubic polynomial $y^3 - ay + b$. Since $y(t) > 0$, by (i), it follows that $y''(t) > 0$ if $\phi(y) = 0$ has no positive root (for then $\phi(y) > 0$ if $y > 0$, since $\phi(\infty) = \infty$). But $\phi(y) = 0$ has no positive root if $4a^3 < 27b^2$. Hence, for reasons of continuity, the assertion

$y''(t) \geqq 0$, of (iii) follows even if the last $<$ is relaxed to $\leqq$. Since the resulting inequality between a and b is precisely the assumption of (iii), the assertion of (iii) follows.

Proof of (iv). Differentiation of (2) shows that $f' = 2yy' - y''$. Hence $f' \leqq 0$ is necessary for (7). But (7) is the assumption of (iv).

* *

*

Let T denote the class of totally monotone functions $z(t)$ on $0 < t < \infty$, characterized by the existence of a Hausdorff-Bernstein integral representation or, equivalently, by the inequalities $(-D)^n z(t) \geqq 0$, where $n = 0, 1, \cdots$. The assertions of (i)-(iii) are that, under their assumptions on $f(t)$ and $f'(t)$, the first three of these inequalities are satisfied by the negative of the logarithmic derivative, $z = y(t)$, of the Kneser solution, $x = x(t)$, of (1). But one can ask whether *all* inequalities $(n = 0, 1, \cdots)$ follows for $z = y(t)$ if *all* of them are assumed for $z = f(t)$; i.e., whether $(f \in T) \Rightarrow (z \in T)$ is true for $z = y$. The question* is the more natural since, as mentioned after (4), the last $\Rightarrow$ is true for $z = x$. But it turns out to be false for $z = y$.

Actually, (I) $f \in T$ is necessary, but not sufficient, for $y \in T$, and the situation becomes just the opposite if (2) is replaced by (1), since (II) $f \in T$ is sufficient, but not necessary, for $x \in T$ (here $x(t)$ and $y(t)$ are Kneser's solution of (1) and the corresponding function (3) respectively).

First, if x is the function $1 + e^{-t}$, then $x \in T$. But $f = x''/x$, by (1), and so $f = e^{-t}/(1 - e^{-t})$ has on $(0, \infty)$ an expansion $c_1 e^{-t} + c_2{}^{-2t} + \cdots$, with $c_n = (-1)^{n-1}$, whereas $c_n \geqq 0$ ought to hold for every n (Hausdorff-Bernstein) if $f \in T$ were true. This proves the second part of (II). The first part of (II) is the result referred to after (4).

Next, if $y \in T$, then $y^2 \in T$ and $-y' \in T$, and so, if (2) is written in the form $f = y^2 - y'$, it follows that $f \in T$, as claimed by the first part of (I). Hence, only the second part of (I) remains to be proved.

To this end, let $y(t)$ be a power series $\Sigma a_n e^{-nt}$ which converges on $(0, \infty)$ (i.e., let $\limsup |a_n|^{1/n} \leqq 1$), choose $a_2 = -1$ but $a_n \geqq 0$ if $n \geqq 3$, and let a_0 and a_1 be positive numbers, the larger the better for the present. In any

* In the second of the notes quoted in the title of this paper, the question $y \in T$ was considered under the assumption that the coefficient function $f(t)$ of (1), instead of being non-negative as above, is non-positive on $(0, \infty)$. This situation is of a somewhat restricted scope, since, while (1) is non-oscillatory in every case $f(t) \geqq 0$, it will be oscillatory in a case $f(t) \leqq 0$ unless $-f(t) \geqq 0$ is "small." But unless (1) is non-oscillatory, it is clear from (3) that (2) will not possess any solution $y(t)$ which exists (as a finite-valued function) on the whole of $(0, \infty)$.

case, let $a_0 + a_1 \geqq 1$. Then $y(t) > 0$ on $(0, \infty)$, as required by (i). But since *not every* a_n is non-negative, it follows from the uniqueness of a Laplace-Stieltjes representation, and from the theorem Hausdorff-Bernstein, that $y \in T$ fails to hold. On the other hand, if $f(t)$ turns out to be a power series $\Sigma c_n e^{-nt}$ in which $c_n \geqq 0$ holds for *every* n, then $f \in T$ will be satisfied. This can however be arranged for, as follows:

Substitution of $y(t) = \Sigma a_n e^{-nt}$ into the formulation $f = -y + y^2$ of (2) shows that $c_0 > 0$ and $c_1 > 0$ (if $a_0 > 0$ and $a_1 > 0$ are large enough), and that $c_n = na_n + \Sigma a_{n-k} a_k$ if $n \geqq 1$, where $0 \leqq k \leqq n$. Since $a_2 = -1$, it is also clear that $c_2 \geqq 0$ (if $a_0 > 0$ and $a_1 > 0$ are large enough), and that $c_n \geqq 0$ will hold for $n \geqq 3$ if and only if

$$na_n + \sum_{k=0}^{n}{}^{*} a_{n-k} a_k \geqq 2a_{n-2}, \qquad (n = 3, 4, \cdots), \tag{9}$$

where the * refers to the omission of both summation indices $k = 2$, $k = n-2$. The contribution of the latter would be $a_2 a_{n-2} + a_{n-2} a_2 = -2a_{n-2}$ but is written on the right of the inequality (9).

Note that no a_m occurring on the left of (9) has the index $m = 2$ and so, since a_2 is the only negative a_m, all terms of the sum Σ^* are non-negative. Hence, if the a-values having an index less than a fixed n have been determined, then, since a_n occurs only on the left of (9), the n-th of the inequalities (9), where $n \geqq 3$, can be satisfied by choosing a_n large enough. The only precaution needed is that the successive choice of the a_n-values should not make them too large, but such as to be compatible with the condition $\limsup a_n^{1/n} \leqq 1$, the condition needed for the convergence of $y(t) = \Sigma a_n e^{-nt}$ on $(0, \infty)$. But it is readily seen from the presence of the large factor $(= n)$ in the first term of (9) that this condition can be satisfied by the successive choice of $a_3 > 0, a_4 > 0, \cdots$, the initial values a_0, a_1 being positive and arbitrarily large, while $a_2 = -1$.

(I) and (II) imply that $f \in T$ is sufficient for $x \in T$ but not for $y \in T$. This contains of course the fact that (without any reference to an f) the definition (3) fails to be such as to lead from $x \in T$ to $y \in T$; but this fact is made trivial by the example $x = 1 + e^{-t}$, since $y \in T$ is prevented by $y = e^{-t}/(1 + e^{-t}) = e^{-t} + be^{-2t} + \cdots$, where $b = -1 < 0$. All that is true is that $y \in T$ is sufficient for $x \in T$ if $x > 0$ (without any reference to an f). For if $x(t)$ is a positive function satisfying a differential equation of the form $x' = -y(t)x$ with some $y \in T$, then, as is well-known, successive differentiations lead, by an induction, from $(-D)^n y \geqq 0$ to $(-D)^n x \geqq 0$.

THE JOHNS HOPKINS UNIVERSITY.

ON THE NON-VANISHING OF EULER PRODUCTS.*

By Norbert Wiener and Aurel Wintner.

Let a function $\chi = \chi_p$, defined on the set of all prime numbers p, be such as to satisfy the following two conditions:

(1) $$-1 \leqq \chi_p \leqq 1$$

(e.g., $\chi_p^2 = |\chi_p|$, i.e., $\chi_p = -1, 0, 1$) and

(2) $$f(s) \text{ is meromorphic on } \sigma = 1,$$

if $f(s)$ the Euler product

(3) $$f(s) = \Pi(1 - \chi_p/p^s)^{-1} \qquad (\sigma > 1).$$

By the condition (2) is meant the assumption that there exist an open domain D in the s-plane and a meromorphic function $f(s)$ on D in such a way that D contains the half-plane $\sigma \geqq 1$ (but possibly no half-plane $\sigma \geqq 1 - \epsilon$, where $\epsilon > 0$) and that $f(s)$ is identical on the half-plane $\sigma > 1$ with the function which is there represented by the product (3); a function which, in view of (1), is regular (and non-vanishing) for $\sigma > 1$. On the other hand, the condition (1) means that if χ is extended from primes to positive integers by the assignments $\chi_1 = 1$ and $\chi_n \chi_m = \chi_{nm}$ (so that (3) becomes identical with the absolutely convergent Dirichlet series $\Sigma \chi_n/n^s$ if $\sigma > 1$), then the resulting real-valued representation χ_n of the multiplication on the semi-group of the positive integers n is a bounded representation (in fact, $\limsup |\chi_n| = \infty$ unless $|\chi_n| \leqq 1$ for every n). The two extreme cases allowed by (1) and (2) result if $\chi_p = 1$ and $\chi_p = -1$ (for every p); in fact, since (3) then reduces to

(4) $$\Pi(1 - p^{-s})^{-1} = \zeta(s) \text{ and } \Pi(1 + p^{-s})^{-1} = \zeta(2s)/\zeta(s),$$

(2) is satisfied in both cases.

The following considerations were suggested by a point occurring in Hadamard's, and also in de la Vallée Poussin's, proof of

(5) $$\zeta(s) \neq 0 \text{ on } \sigma = 1.$$

* Received June 29, 1957.

The point in question is the following: Besides the case $f(s) = \zeta(s)$ of (2), it is assumed in the proof of (5) that $\zeta(s)$ *is regular* (*rather than just meromorphic*) *at every* $s = 1 + it \neq 0$. It is this fact from which the negation of (5) leads to a contradiction, since what is actually proved is the following: If $\zeta(s)$ would have a zero $s = 1 + it_0$, then it would also have some pole $s = 1 + it^0$ distinct from the pole $s = 1$ (in fact, it is shown that t^0 could be chosen to be $2t_0$; cf., e.g., [1], pp. 29-30). Accordingly, the proof of (5) fails to succeed if all that is known for the case $f(s) = \zeta(s)$ of (3) is the following pair of assumptions: (2) and

(6) $$f(s) \text{ has a pole at } s = 1.$$

There is quite another proof of (4), the function-theoretical proof adapted by Ingham from Landau's proof [2] of Dirichlet's theorem $L(1) \neq 0$ (in Landau's function-theoretical proof, $L(s)$ belongs to a real character); cf. [1], p. 89. But this proof is even more restrictive than the preceding one, since what is now assumed is the regularity of $f(s)$ at every point $s \neq 1$ of the half-plane $\sigma \geqq \frac{1}{2}$ (on the boundary line $\sigma = \frac{1}{2}$, less than regularity is needed).

Thus it is natural to ask whether

(7) $$f(s) \neq 0 \text{ on } \sigma = 1,$$

the generalization of (5) for an arbitrary case (1) of (3), must or need not be true if only (2) and (6) are assumed. For, as seen above, the classical argument applies only if (1) is retained but (2) is strengthened to the hypothesis that

(8) $$f(s) \text{ is regular on } \sigma = 1 \text{ if } s \neq 1.$$

The purpose of this note is to show that the answer to the question, just raised, is in the affirmative; in other words, that (7) remains true if (8) is relaxed to (2). Curiously enough, (8) proves to be a consequence of the other hypotheses; so that the situation is as follows:

(I) *In terms of a sequence* $\chi_2, \chi_3, \cdots$ *satisfying* (1), *define on the open half-plane* $\sigma > 1$ *a* (*regular, non-vanishing*) *function* $f(s)$ *by the corresponding Euler product* (3), *and suppose that, as* $\sigma \to 1 + 0$, *the function* $f(s)$ *behaves in such a way that conditions* (2) *and* (6) *are satisfied. Then both* (8) *and* (7) *hold.*

Actually, (I) is not the final result, since the assumption (6) of (I)

proves to be superfluous. This is the content of the theorem at the end of this paper.

Although (I) contains (5), there will result no new proof of (5), since (5), along with

$$1/\zeta(s) \neq 0 \text{ on } \sigma = 1 \text{ if } s \neq 1 \tag{9}$$

(that is to say, the regularity and the non-vanishing of $\zeta(1+it)$ for $0 < t < \infty$), will be granted in the proof of (I). What will directly be proved is not (I) itself but the following variant of (I):

(II) *The assertions of* (I) *remain true if its assumption* (6) *is replaced by the assumption*

$$f(1) = 0 \tag{10}$$

(and all the other assumptions of (I) are retained).

Proof of (II). For $-\infty < t < \infty$, let j_t denote the index (the logarithmic residue) of $f(s)$ at $s = 1 + it$, and let J_t belong to

$$F(s) = \zeta(s) f(s) \tag{11}$$

in the same way as j_t belongs to $f(s)$. Since (2) is assumed for $f(s)$ itself and for $f(s) = \zeta(s)$, it is clear from (5), (9) and (11) that $j_t = J_t$ for $t \neq 0$. Since the assertions, (8) and (7), of (II) are equivalent to $j_t = 0$ for $t \neq 0$, and since (10) and (11) imply that $J_0 = 0$ (for $\zeta(s)$ has a simple pole at $s = 1$), it follows that (II) will be proved if it is shown that

$$|J_t| \leqq J_0 \qquad (J_0 = 0) \tag{12}$$

holds for every t. But the truth of (12) can be concluded by an elementary argument (cf. [3], where (8), rather than just (2), is assumed, (10) is retained, and (1) is generalized to complex-valued χ_p, with $|\chi_p| \leqq 1$).

In order to prove (12), note that, if $\sigma > 1$, logarithmic differentiation of (3) leads to

$$-f'/f(s) = \sum_p \sum_{k=1}^{\infty} (\chi_p \log p)/p^{ks}. \tag{13}$$

If (13) is added to the case $\chi_p = 1$ of (13), it follows from (11) and from the first of the relations (4) that, if $\sigma > 1$,

$$-F'/F(s) = \sum_p \sum_{k=1}^{\infty} a_p/p^{ks}, \tag{14}$$

where

(15) $$a_p = (1 + \chi_p) \log p.$$

But since (15) and (1) imply that $a_p \geqq 0$, it is clear from (11) that, if $\sigma > 1$,

(16) $$|(\sigma - 1)F'/F(\sigma + it)| \leqq |(\sigma - 1)F'/F(\sigma)| \text{ for } -\infty < t < \infty.$$

If $\sigma \to 1 + 0$, then (16) goes over into $|J_t| = |J_0|$, and so (12) follows from the parenthetical equality in (12).

This completes the proof of (II).

Actually, the following extension of (II) was also proved:

(II*) *The assertions of* (II) *remain true if its assumption* (1) *is replaced by the unilateral restriction* $-1 \leqq \chi_p$, *provided that the Euler product* (3) *is uniformly convergent on every compact subset of the half-plane* $\sigma > 1$.

The latter proviso (which, since χ_p is bounded from below, is satisfied if, though not only if, $\chi_p \leqq$ Const. for some Const.) cannot of course be omitted. But then the restriction $-1 \leqq \chi_p$ will suffice in the preceding proof, since, in view of (15), this unilateral restriction is equivalent to $a_p \geqq 0$.

Much deeper lies the following fact:

(II bis) *Under the assumptions of* (II), *and even those of* (II*), *the function* $f(s)$ *possesses an analytic continuation which is meromorphic on some half-plane* $\sigma > 1 - \epsilon$, *where* $\epsilon = \epsilon_f > 0$, *and* $f(s)$ *does not vanish at any point* $s \neq 1$ *of this half-plane* $\sigma > 1 - \epsilon$.

[REMARK. *If it is true that* $\zeta(s)$ *has no zero on some open half-plane containing the line* $\sigma = 1$ (*for instance, if Riemann's hypothesis is true*) *then, in* (II bis), *the word "meromorphic" can be replaced by "regular."*]

In fact, since $\zeta(s)$ has a simple pole at $s = 1$, it is clear from (2), (10) and (11) that, if $\epsilon > 0$ is small enough, $F(s)$ is regular at every point of the half-line $s > 1 - \epsilon$, and that $F(s)$ can have a zero on such a half-line only if $s = 1$ is a multiple zero of $f(s)$ (in fact, (3) does not vanish for $s > 1$). But $f(s)$ cannot have a multiple zero at $s = 1$, since, if $s > 1$ and $-1 \leqq \chi_p$, it is clear from (3) that

$$f(s) \geqq \Pi(1 + p^{-s})^{-1} \sim \text{const.}\ (s - 1) \text{ as } s \to 1 - 0,$$

where const. $= \zeta(2) > 0$, by the second of the relations (4).

Accordingly, $F(s)$ is a regular and non-vanishing function, and so the logarithmic derivative of $F(s)$ is a regular function, on some half-line $s > 1 - \epsilon$. Since $a_p \geqq 0$, it now follows from Landau's theorem (on Dirichlet series $\Sigma\, c_n/n^s$ with $c_n \geqq 0$), a theorem referred to but not used above, that the Dirichlet series (14) must converge for $s > 1 - \epsilon$ and, therefore, for $\sigma > 1 - \epsilon$. Consequently, the logarithmic derivative of $F(s)$ is a regular function, and therefore $F(s)$ is a non-vanishing regular function, on the half-plane $\sigma > 1 - \epsilon$. In view of (11), this proves both (II bis) and the Remark following (II bis).

Proof of (I). If χ_p is replaced by $-\chi_p$ (for every p), then the assumption (1) remains unaltered but (3) becomes replaced by

(17) $$f^*(s) = \Pi(1 + \chi_p/p^s)^{-1}.$$

The connection between (3) and (17) is involutory. But while it is clear from (1) that (17) represents a non-vanishing regular function for $\sigma > 1$, it is not quite obvious that (2), too, is an involutory property; in other words, that

(18) $$f^*(s) \text{ is meromorphic on } \sigma = 1$$

if (2) is assumed. It turns out, however, that (18) follows from (2) and is, therefore, equivalent to (2).

First, since (2) remains true if $f(s)$ is replaced by $1/f(s)$, more than (18) will follow if it is ascertained that the quotient of $f^*(s)$ and $1/f(s)$ is a non-vanishing regular function on the line $\sigma = 1$. But (3) and (17) show that, if $\sigma > 1$, this quotient is identical with

(19) $$f(s)f^*(s) = \Pi(1 - \chi_p^2/p^{2s})^{-1}.$$

On the other hand, it is clear from (1) that (19) is a regular and non-vanishing function on the half-plane $\sigma > \frac{1}{2}$ and, therefore, on the line $\sigma = 1$. [This conclusion is curious, since, by placing either $\chi_p = 1$ or $\chi_p = 0$, and making the alternative choice in an appropriate ("lacunary") manner, it is easy to obtain a pair of functions (1), (17), the factors on the left of (19), which are regular on the half-plane $\sigma > \theta$ but become singular at every point of the line $\sigma = \theta$, where $\frac{1}{2} < \theta < 1$, rather than $\theta = \frac{1}{2}$.]

Let (1*), (2*), $\cdots$ denote what results if $f(s)$ is replaced by $f^*(s)$, and χ_p by $-\chi_p$, in (1), (2), $\cdots$ respectively. Then, as just shown, (1) and (2) together are equivalent to (1*) and (2*) together. Since (II) has already been proved, it follows that (1*), (2*) and (10*) imply both (8*) and (7*).

But the quotient of $f^*(s)$ and $1/f(s)$ and, hence, the quotient of $1/f(s)$ and $f^*(s)$, was seen to be a non-vanishing regular function on the line $\sigma=1$. Hence (8*) and (7*) are equivalent to (7) and (8) respectively and so, since (10) goes over into (6) if $f(s)$ is replaced by $1/f(s)$, the proof of (I) is now complete.

* *
*

If $f(s)$ is an L-function of Dirichlet belonging to a real non-principal character (so that, in particular, (1) and (3) hold for a certain χ_p which is capable of the three values $-1, 0, 1$ only), and if the meromorphic (rather than the regular) behavior of $L(s)$ on $\sigma=1$ is assumed, then, since $L(1)\neq 0$ (Dirichlet) but $L(1)\neq\infty$, neither the non-vanishing nor the regularity of $L(s)$ on $\sigma=1$ can be concluded from (I) and (II) together. Hence there arises the question whether or not (7) and (8) remain true if (1) and (2) are retained for (3) but (6) and (10) are replaced by

$$0\neq f(1)\neq\infty \tag{20}$$

(or, what in view of (1) and (3), where $\sigma>1$, is the same thing, by $0<f(1)<\infty$). It will be shown that the answer to this question is affirmative:

(III) *The assertions of* (I) *remain true if* (6) *is replaced by* (20).

In order to prove (III), it will be sufficient to show that, under the assumptions of (III), the line $\sigma=1$ cannot contain a zero of $f(s)$. For if this is granted, then the remaining assertion of (III), according to which $f(s)$ cannot have a pole on $\sigma=1$, will follow in the same way in which (I) and (II) were proved to be equivalent (that is, by applying (17) and (19) in the same way as above). Hence it is sufficient to assume that $f(s)$ has a zero $s=1+ia$ on $\sigma=1$ and to show that the existence of at least one such real number a leads to a contradiction.

First, $a\neq 0$, since $f(1)\neq 0$. Next, since $f(s+ia)=0$ at $s=1$, and since (1) and (3) imply that $f(1+it)$ and $f(1-it)$ are complex conjugate values, it is clear that the function

$$G(s)=\zeta^2(s)f(s+ia)f(s-ia) \tag{21}$$

(which, in view of (2), is meromorphic on $\sigma=1$) will have at $s=1$ neither a zero nor a pole if the zero $s=1+ia$ of $f(s)$ is a simple zero (the factor $\zeta^2(s)$ of (21) has a double pole at $s=1$). But the argument applied in the

proof of (II bis) also shows that $f(s)$ cannot have a multiple zero on $\sigma=1$ (simply because (1) and (3) imply that, if $\sigma>1$,

$$|f(\sigma+it)|\geqq\Pi(1+p^{-})^{-1}=\zeta(2\sigma)/\zeta(\sigma)>\text{Const.}(\sigma-1)$$

holds for every t and for a certain Const. >0). Accordingly, if K_t denotes the logarithmic residue of $G(s)$ at the point $s=1+it$, then $K_0=0$.

It will be shown that

$$(22)\qquad |K_t|\leqq|K_0|$$

holds for every t. In view of $K_0=0$, this will prove that $K_t=0$ holds for every t. It will therefore follow from (5), (9) and (21) that $f(s+ia)f(s-ia)$ is of index 0, and so a non-vanishing regular function, at every point $s\neq 1$ of the line $\sigma=1$. Since $f(1+it)$ and $f(1-it)$ are complex conjugates, and since $a\neq 0$, it now follows that $f(s)$ is regular (rather than just meromorphic) on $\sigma=1$. But since $s=1+ia$ and $s=1-ia$ are two distinct zeros of $f(s)$, this contains a contradiction. In fact, it was shown in [3] that if (1) (or, in the complex case, just $|\chi_p|\leqq 1$) holds in (3), where $\sigma>1$, and if the function $f(s)$ remains regular at every point of $\sigma=1$, then $f(s)$ cannot have more than one zero on $\sigma=1$.

In view of this contradiction, the proof of (III) will be complete if the truth of (22) is proved (for every t). But (22) can be proved, along the lines of the proof of (12), as follows:

If $s=\sigma+it$, where $\sigma>1$, is replaced in (13) once by $s+ia$ and once by $s-ia$, it follows, by addition, that the logarithmic derivative of $f(s+ia)f(s-ia)$ is

$$(23)\qquad -\sum_p\sum_{k=1}^{\infty}(\lambda_{p,k}\log p)/p^{ks},\text{ where }\lambda_{p,k}=2\chi_p\cos(ak\log p).$$

On the other hand, it follows from the first of the relations (4) that the logarithmic derivative of $\zeta^2(s)$ results from (23) if χ_p and a are replaced by 1 and 0 respectively. If the resulting series is added to (23) itself, then the definition, (21), of $G(s)$ shows that

$$(24)\qquad -G'/G(s)=\sum_p\sum_{k=1}^{\infty}b_{p,k}/p^{ks}\text{ for }\sigma>1,$$

where

$$(25)\qquad b_{p,k}=2\mu_{p,k}\log p,\qquad \mu_{p,k}=1+\chi_p\cos(ak\log p).$$

But it is seen from (25) and (1) that $b_{p,k}\geqq 0$. Hence it is clear from (24)

that (16) remains true if F is replaced by G. Consequently, (22) follows by letting $\sigma - 1 \to +0$.

Since this completes the proof of (III), the final result is as follows:

THEOREM. *If there is assigned to every prime p a value χ_p satisfying $-1 \leqq \chi_p \leqq 1$, and if the function $f(s)$, defined for $\sigma > 1$ by the Euler product $f(s) = \Pi(1 - \chi_p/p^s)^{-1}$, remains meromorphic at every point of the line $\sigma = 1$, then $f(s)$ is a regular and non-vanishing function at every point $s \neq 1$ of the line $\sigma = 1$.*

This theorem, which is equivalent to (I), (II) and (III) together, can be completed by the further information supplied by (II bis) and (II*) [and also by the hypothetical information contained in the Remark formulated after (II bis)].

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] A. E. Ingham, *The distribution of primes*, Cambridge Tracts, no. 30, 1932.

[2] E. Landau, "Ueber einen Satz von Tschebyscheff," *Mathematische Annalen*, vol. 61 (1905), pp. 527-550.

[3] A. Wintner, "On the non-vanishing of certain Dirichlet series," *American Journal of Mathematics*, vol. 74 (1952), pp. 723-725.

LOCAL CONTRACTIONS AND A THEOREM OF POINCARÉ.* [1]

By SHLOMO STERNBERG.

One of the earliest treatments of the problem of normal forms for a system of n differential equations at a singular point occurs, at least implicitly, in Poincaré's thesis [6], pp. XCIX-CV (cf. also Picard [5]). In his thesis, Poincaré is concerned with those analytic partial differential equations of first order for which the Cauchy-Kowalewsky theorem does not apply. An important lemma in his considerations is the following: Given n analytic functions X_i of n complex variables x_j which are defined in some neighborhood of the origin and such that $X_i = \lambda_i x_i +$ higher order terms, consider the partial differential equations

$$X_1 \partial y_j/\partial x_1 + X_2 \partial y_j/\partial x_2 + \cdots + X_n \partial y_j/\partial x_n = \lambda_j y_j. \tag{1_j}$$

Then if

(i) all the λ_i lie in the same open half-plane about the origin

and

(ii_j) $\lambda_j \neq \sum m_i \lambda_i$ for any non-negative integral m_i such that $\sum m_i > 1$,

equation (1_j) has an analytic solution in some neighborhood of the origin. Now (1_j) is the j-th partial differential equation that a change of coordinates

$$y_i = y_i(x_1, x_2, \cdots, x_n) \qquad (i = 1, 2, \cdots, n) \tag{2}$$

must satisfy in order that it transform the system of ordinary differential equations

$$dx_i/dt = X_i(x_1, x_2, \cdots, x_n) \tag{3}$$

into the linearized form

$$dy_i/dt = \lambda_i y_i. \tag{4}$$

---

* Received March 11, 1957.

[1] This paper was written while the author was a Temporary Member of the Institute of Mathematical Sciences, New York University, during the academic year 1956-57. This Temporary Membership Program is supported by the National Science Foundation. Reproduction in whole or in part permitted for any purpose of the United States Government.

Thus if we denote by (ii) the totality of conditions (ii_j) for all j we can rephrase Poincaré's theorem as follows: Given a system of analytic differential equations (3) defined near the origin such that $X_i(0,0,\cdot\cdot\cdot,0)=0$ and whose matrix of linear terms is diagonizable with eigenvalues λ_i satisfying (i) and (ii), then there exists an analytic change of coordinates (2) transforming (3) into (4).

Poincaré's proof of this theorem is a straightforward application of the Cauchy majorant method; condition (ii) implies the existence of a formal power series solution and (i) implies convergence. In this paper we shall deal with the problem of normal forms for real non-analytic differential equations for which there is, of course, no majorant method. Our approach will be of a geometrical nature and will deal with the flow generated by (3) rather than with (3) itself. If we examine condition (i) for the case of real differential equations, we observe that since every complex eigenvalue occurs along with its complex conjugate, the only admissible half planes are the right and left half planes. Substituting $-t$ for t, if necessary, we can replace (i) by

$$(\mathrm{i}_R) \qquad \operatorname{Re}\lambda_j < 0 \quad \text{for all } j.$$

But (i_R) implies that the flow generated by (3) is a one-parameter semigroup of contractions in some neighborhood of the origin, i. e., that all points sufficiently close to the origin tend to the origin with increasing time. In what follows we shall obtain normal forms for smooth contractions in Euclidean n-space, that is, we shall obtain invariants for C^n contractions under inner automorphisms of the group of local C^k changes of coordinates. In addition to supplying information on the problem of normal forms for differential equations, our results generalize (to n dimensions and the non-analytic case) certain results of Lattès [3] on analytic surface transformations. We shall also obtain a generalization of the results of [8] on invariant curves to n dimensions.[2]

2. Before dealing with the problem of normal forms for contractions, we shall show that the problem is of an entirely different nature if no smoothness assumptions are made. This remark which is not essential in the sequel, follows from the fact that any two orientation preserving contractions in n-space are equivalent if the group of orientation preserving homeomorphisms of the $(n-1)$-sphere is arc-wise connected. This property

[2] These results are an outgrowth of ideas contained in my thesis which was written under the direction of Professor Wintner.

is trivial for spheres of zero and one dimensions and is assured by a known theorem of H. Kneser in two dimensions. If there exists an n not satisfying the above condition, then the statement of Theorem 1 would have to be modified to take this fact into account. At any event, the structure of the mapping of the n-sphere has no effect on the following paragraphs.

THEOREM 1. *Let S and T be two orientation preserving homeomorphisms of some neighborhood of the origin in Euclidean n-space into itself such that*

$$\| Sx \| < \| x \| \text{ and } \| Tx \| < \| x \|, \tag{5}$$

where $\| \cdot \|$ is the ordinary Euclidean norm and where n satisfies the conditions preceding the theorem. Then there exists a homeomorphism R of some neighborhood of the origin onto itself keeping the origin fixed and such that

$$RSR^{-1} = T. \tag{6}$$

Proof. Let $\mathcal{S}$ denote some sphere which, together with its interior, $\mathcal{B}$, is contained in the domain of definition of S and T. In virtue of (5)

$$T^{n+1}(\mathcal{B}) \subset T^n(\mathcal{B}) \text{ and } S^{n+1}(\mathcal{B}) \subset S^n(\mathcal{B})$$

so that we can write

$$\mathcal{B} = \cup (T^n(\mathcal{B}) - T^{n+1}(\mathcal{B})) \text{ and } \mathcal{B} = \cup (S^n(\mathcal{B}) - S^{n+1}(\mathcal{B})). \tag{7}$$

We define R to be the identity map on $\mathcal{S}$ and to map $\mathcal{B} - S(\mathcal{B})$ homeomorphically onto $\mathcal{B} - T(\mathcal{B})$ in such a manner that $R(Sx) = Tx$ for all x on $\mathcal{S}$. This can clearly be done since S and T are both homeomorphisms and by the assumptions concerning n. We now define R inductively to map $S^n(\mathcal{B}) - S^{n+1}(\mathcal{B})$ onto $T^n(\mathcal{B}) - T^{n+1}(\mathcal{B})$ by the equation

$$RS = TR. \tag{8}$$

If we set $R(0) = 0$ then, by (7) R is defined on all of $\mathcal{B}$. Furthermore, since R was defined so as to be continuous at $S(\mathcal{S})$, it is a homeomorphism of $\mathcal{B}$ onto itself satisfying (8), and hence (6) proving the theorem.

3. As soon as we restrict our group of local changes of variable to be of class C^1, Theorem 1 becomes false. In fact, there is a natural homomorphism of the group of local C^1 homeomorphisms onto the group of all non-singular n by n matrices: $T \rightarrow J(T)$ where $J(T)$ is the Jacobian matrix of the transformation T at the origin. The next conjecture would be that

a normal form for $J(T)$ would be a suitable normal form for T. Now for the one dimensional case it was shown in [9] that if the linear operator $J(T)$ is a contraction and T is of class C^{k+1} $(k \geqq 1)$ then T can be linearized by a change of coordinates of class C^k. However this is not true in the n-dimensional case. In fact we shall exhibit an analytic contraction of the plane which can not be linearized by any transformation of class C^2 having a non-vanishing Jacobian at the origin. Consider the transformation

$$x_1 = a^2x + y^2, \qquad y_1 = ay. \tag{9}$$

We wish to show that there is no C^2 transformation

$$\xi = f(x,y), \qquad \eta = g(x,y) \tag{10}$$

such that in the ξ, η coordinates (9) assume the form

$$\xi_1 = a^2\xi, \qquad \eta_1 = a\eta. \tag{11}$$

In order for (10) to transform (9) into (11) f must satisfy the functional equation

$$f(a^2x + y^2, ay) = a^2f(x,y). \tag{12}$$

taking the partial derivative of both sides of (12) with respect to y gives

$$2yf_x(a^2x + y^2, ay) + af_y(a^2x + y^2, ay) = a^2f_y(x,y). \tag{13}$$

Setting $x = y = 0$ in (13) yields

$$f_y(0,0) = 0. \tag{14}$$

Differentiating (13) with respect to y and setting $x = y = 0$ gives

$$f_x(0,0) = 0. \tag{15}$$

But (14) and (15) imply that the Jacobian of (10) vanishes at the origin. Thus (9) can not be linearized.

4. In the n-dimensional case, the problem of finding normal forms for smooth transformation splits into two parts: one of a purely formal nature and the other analytic in character. In this section we shall deal with the formal part; our main goal being to bring every transformation satisfying certain formal conditions analogous to (i) into a prepared form so that the analytic considerations of the following section apply. Before proceeding with the calculations we shall make some remarks about the formalism in

general. Let T^k denote the set of all C^k homeomorphisms defined in some neighborhood of the origin in n space keeping the origin fixed and having a non-vanishing Jacobian there. Given any two transformations A and B in T^k, we can compose them to form a third transformation $C = B \cdot A$ in T^k provided that we restrict attention to a sufficiently small neighborhood N of the origin. In order to be able to define C on N, N must be contained in the domain of A and such that $A(N)$ is contained in the domain of B. In order to avoid such difficulties, we can introduce the equivalence relation '$A \equiv B$ if A is identical with B on some sufficiently small neighborhood of the origin.' The elements of the coset space of T^k with respect to this equivalence relation form a group G^k known as the group of local C^k transformations. Now let P^k $(1 \leqq k \leqq \infty)$ denote the set of n-tuplets of real polynomials (formal power series) without constant terms in n real variables, which have terms of degree at most k. Then $P^1 \subset P^2 \subset \cdots \subset P^k \subset \cdots \subset P^\infty$. Let $\mathcal{J}^k$ denote the operator which truncates the n-tuplets of formal power series at their terms of degree k;

$$\mathcal{J}^k(\cdot\ \cdot\ \cdot, \sum_{i_j=1}^{\infty} a^i_{i_1\cdots i_n} x_1^{i_1} \cdot\ \cdot\ \cdot x_n^{i_n}, \cdot\ \cdot\ \cdot)$$
$$= \mathcal{J}^k(\cdot\ \cdot\ \cdot, \sum^{i_1+\cdots i_n \leqq k} a^i_{i_1\cdots i_n} x_1^{i_1} \cdot\ \cdot\ \cdot x_n^{i_n}, \cdot\ \cdot\ \cdot).$$

Then P^k has a natural multiplication defined on it, namely substitution followed by truncation of order k. If F^k denotes those elements of P^k whose matrix of linear terms is non-singular, then F^k is a group under this multiplication. The truncation operator $\mathcal{J}^k$ provides a canonical homomorphism of F^s onto F^k for $s > k$. Furthermore there is a natural homomorphism of G^k onto F^k once coordinates are chosen in Euclidean space, given by sending every mapping

$$(x_1, \cdot\ \cdot\ \cdot, x_n) \to (f_1(x_1, \cdot\ \cdot\ \cdot, x_n), \cdot\ \cdot\ \cdot, f_n(x_1, \cdot\ \cdot\ \cdot, x_n))$$

into the n-tuple whose elements are the Taylor expansions of the f_i at the origin of order k. We will now state a sufficient condition for an element of F^k to be linearizable by inner automorphisms of F^k. Since the mapping T^k is a homomorphism onto, it is sufficient for us to prove the result for F^∞.

LEMMA 1. *Let T be an element of F^k whose matrix of linear terms has no multiple elementary divisors and whose (possibly complex) eigenvalues $s_1, s_2, \cdot\ \cdot\ \cdot, s_n$ satisfy*

(II) $s_i \neq s_1^{m_1} s_2^{m_2} \cdot\ \cdot\ \cdot s_n^{m_n}$ *for any non-negative integral m_j such that*

$$\sum m_j > 1.$$

Then T is equivalent to its matrix of linear terms by an inner automorphism of F^k.

Since our groups are real, if complex eigenvalues do occur, they occur in pairs of complex conjugates. In that case, it is convenient to modify the group F^k by replacing the pair of real coordinates corresponding to the complex eigenvalues by a pair of conjugate complex variables and to allow complex formal power series satisfying certain symmetry (reality) conditions. This procedure is explained in detail in Birkhoff [1], pp. 60-63. In what follows, these symmetry conditions are automatically verified for the series that arise in virtue of the method of their construction. The convenience of introducing the complex coordinates is, of course, that it allows us to diagonalize the matrix of linear terms. We thus assume that T has the form

$$(s_1x_1 + \sum t^1_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n},\cdots, s_nx_n + \sum t^n_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}),$$

where all the series start with terms of degree at least two. We wish to find an $R = (r_1,\cdots,r_n)$ where the r_i are formal power series such that $RTR^{-1} = S = (s_1x_1,\cdots,s_nx_n)$. We can assume that the matrix of linear terms of R is the identity matrix and rewrite the desired equation as $RT = SR$ or

$$\begin{aligned} &s_i(x_i + \sum r^i_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}) \\ (16)\qquad &= s_ix_i + \sum r^i_{i_1\cdots i_n}(s_1x_1)^{i_1}\cdots(s_nx_n)^{i_n} + \sum t^i_{j_1\cdots j_n}x_1^{i_1}\cdots x_n^{i_n} \\ &\quad + R_i(\sum t^1_{j_1\cdots j_n}x_1^{i_1}\cdots x_n^{i_n},\cdots,\sum t^n_{j_1\cdots j_n}x_1^{i_1}\cdots x_n^{i_n}), \end{aligned}$$

where the $r_i = x_i + \sum r^i_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n} = x_i + R_i$. If we compare the coefficients of $x_1^{i_1}\cdots x_n^{i_n}$ in (16), we obtain

$$(17)\qquad s_ir^i_{i_1\cdots i_n} = (s_1^{i_1}\cdots s_n^{i_n})r^i_{i_1\cdots i_n} + P^i_{i_1\cdots i_n},$$

where $P^i_{i_1\cdots i_n}$ is a polynomial in those $r^j_{j_1\cdots j_n}$ such that $\sum j_k < \sum i_k$. By (II), we can solve (17) for $r^i_{i_1\cdots i_n}$. This allows us to determine consecutively all the coefficients of the r_i so as to satisfy (16), proving the lemma.

5. In this section we shall deal with the analytic aspects of the problem of linearization. We shall therefore have to make an assumption analogous to (i): An element T of T^k will be called a contraction if the eigenvalues, $s_1, s_2,\cdots,s_m$, of $J(T)$ satisfy

$$(\mathrm{I})\qquad |s_i| < 1.$$

In all the cases we shall treat, we assume, for simplicity that the matrix

$J(T)$ has no multiple elementary divisors. Hence, in the coordinate system corresponding to the eigenvectors of $J(T)$, (I) takes the form

$$\text{(I*)} \qquad \| J(T) \| < 1,$$

where the norm is the ordinary Euclidean norm: $\| J(T) \| = \sup \| J(T) \cdot (x) \|$ where the sup is taken over all vectors (x) such that $\| (x) \| = 1$, with $\| (x) \| = \sum x_i^2$ if x_i are the coordinates of (x) in this coordinate system. If S and s denote $\max s_i$ and $\min s_i$ respectively, then

$$\text{(I**)} \qquad s \| (x) \| < \| J(T)(x) \| < S \| (x) \|.$$

Then we have

THEOREM 2. *Let T be a transformation in T^k satisfying* (I) *and* (II) *and such that*

$$(18) \qquad k > \log s / \log S,$$

then there exists a transformation R in T^k such that RTR^{-1} is linear.

In proving this theorem we shall use the method described in [10]. That is, denoting by L the linear transformation which is given by the Jacobian matrix $J(T)$ at the origin, we wish to find an R such that $RTR^{-1} = L$. We rewrite this equation as

$$(19) \qquad R = L^{-1} R T.$$

We shall solve (19) by a process of successive approximations. This process will converge provided that we are able to start with an initial R which satisfies (19) up to terms of sufficiently high order. Such an R will be supplied by Lemma 1. In order to formulate the convergence proof, it is convenient to introduce the following notation. Let $V^k{}_N$ denote the space of n-tuplets $f = (f^1, \cdots, f^n)$ of functions of n real variables defined in some neighborhood N of the origin, which are of class C^k there and which vanish at the origin together with all partial derivatives of order $\leqq k$. Thus $V^j{}_{N'} \subseteq V^k{}_N$ for $N' \supseteq N$ and $j \geqq k$. On the space $V^k{}_N$ we introduce the metric

$$(20) \qquad \| f \|^k{}_N = \sup_N \sum_{i=1}^n \sum_{i_j=1}^n (f^i{}_{x_{i_1} \cdots x_{i_n}})^2.$$

Then an immediate consequence of the above definitions is

LEMMA 2. *Given any f in $V^k{}_N$ and any positive number ϵ, we can find a sufficiently small neighborhood N^ϵ such that*

$$(21) \qquad \| f \|^1{}_{N^\epsilon} + \| f \|^2{}_{N^\epsilon} + \cdots + \| f \|^{k-1}{}_{N^\epsilon} < \epsilon \| f \|^k{}_{N^\epsilon}.$$

Now define the operator $\mathfrak{D}_T$ on $V^k{}_N$ by

$$\mathfrak{D}_T\colon f(\cdot) \to J(T)^{-1} f(T(\cdot)) \tag{22}$$

The essence of the convergence proof is then contained in

LEMMA 3. *Let f be in $V^k{}_N$ and T in T^k with k satisfying* (18). *Then there exists a neighborhood N' of the origin such that*

$$\| \mathfrak{D}_T f \|^k{}_{N'} < K \| f \|^k{}_{N'} \tag{23}$$

for some $K < 1$.

If we call $(t^i{}_j(x))$ the Jacobian matrix of the transformation T at the point x, then for any function f of class C^k on N

$$[f(T(x))]_{x_{j_1}\cdots x_{j_k}} = \sum f_{x_{j_1}\cdots x_{j_k}}(T(x)) t^{j_1}{}_{i_1}(x) \cdot \cdot \cdot t^{j_k}{}_{i_k}(x) + P, \tag{24}$$

where P is a polynomial in derivatives of f of order lower than k, and in derivatives of the $t^i{}_j$ (of order $\leqq k$). Since T is smooth near the origin (I**) implies that we can choose N^δ so that $\| (t^i{}_j(x) \| < S + \delta$ for all x in N_δ. If M denotes the maximum of the derivatives of the $t^i{}_j(x)$ occurring in P for all x in N, set $\gamma = \epsilon / M$. Then by Lemma 2, and (24)

$$\| \mathfrak{D}_T f \|_{N^\gamma \cap N_\delta} < s^{-1}[(S+\delta)^k + \epsilon] \| f \|_{N^\gamma \cap N_\delta}. \tag{25}$$

In view of (18), we can choose δ and ϵ so small that (25) reduces to (23).

In order to complete the proof of Theorem 2 we observe that Lemma 1 implies the existence of an R_0 such that $R_0 - L^{-1}RT$ is in $V^k{}_N$. Then Lemma 3 implies that the sequence of transformations

$$R_n = L^{-n} R_0 T^n = \sum_{k=0}^{n-1} \mathfrak{D}_T{}^k (L^{-1} R_0 T - R)$$

is uniformly convergent and tends to a transformation R in T^k, which clearly satisfies (19), in some neighborhood N^* of the origin.

It should be remarked that although we have defined R only on some small neighborhood N^*, we can extend the definition to any neighborhood N for which T is defined and for which $T^r(N) \subset N^*$ for some suitably large r. In fact, all we have to do is to replace R by $L^{-r}RT^r$. It should also be noted that the above proof is valid in the real analytic case, where it supplies an analytic change of coordinates R.

6. In the last section we proved that any smooth contraction T (and hence the discrete group T^n generated by T) satisfying certain conditions

can be linearized. In this section we show how to pass from the discrete case to that of a continuous one-parameter group. Here there are two smoothness considerations: smoothness of the individual transformations and of their time dependence. In what follows both considerations become trivial in virtue of the general principle enunciated in

LEMMA 4. *Let T_t be a continuous one parameter family of transformations in T^k such that T_n is linear for integral n. Then there exists a transformation R in T^k such that*

$$RT_tR^{-1} = L_t, \tag{26}$$

where L_t is the one-parameter group of linear transformations whose matrices are the Jacobians of T_t at the origin.

In fact set

$$R = \int_0^1 L_{-\alpha}T_\alpha\,d\alpha. \tag{27}$$

Now

$$L_{-t}R = \int_0^1 L_{-\alpha-t}T_\alpha\,d\bar{\alpha} = \int_{-t}^{1-t} L_{-\alpha}T_{\alpha+t}\,d\alpha = \int_{-t}^{0} + \int_0^{1-t}.$$

Then, since $L_{-1}T_1 =$ identity,

$$\int_{-t}^{0} L_{-\alpha}T_{\alpha+t}\,d\alpha = \int_{-t}^{0} L_{-\alpha}(L_{-1}T_1)T_{\alpha+t}\,d\alpha = \int_{1-t}^{1} L_{-\alpha}T_{\alpha+t}\,d\alpha.$$

Thus

$$L_{-t}R = \int_0^1 L_{-\alpha}T_{\alpha+t}\,d\alpha = RT_t$$

or R satisfies (26). It is clear from (27) that R satisfies the smoothness requirements and that $J(R)$ is the identity so that R is in T^k.

Now for any one-parameter group, conditions (I) and (II) are independent of the parameter. If they are satisfied for a group of transformations of class T^k where k satisfies (18) (which is also independent of he parameter), we can first linearize a discrete subgroup by Theorem 1, and then the whole group by Lemma 4. Thus we have proved

THEOREM 3. *Let T_t be a continuous one parameter family of contractions s $(T_{s+t} = T_sT_t)$ which satisfy* (I) *and* (II) *and are of class T^k where k satisfies* (18). *Then there exists a change of coordinates R in T^k which linearizes T_t.*

7. We now translate Theorem 3 into a theorem about differential equations. Consider a system of differential equations (3) where the X_i are functions of class C^k defined in some neighborhood of the origin with $X_i(0,\cdot\cdot\cdot,0)=0$. Then the existence theorem for ordinary differential equations states that there is unique solution

$$x_i(t,\xi) \text{ such that } x_i(0,\xi)=\xi_i, \tag{28}$$

where $\xi=(\xi_1,\cdot\cdot\cdot,\xi_n)$ are the initial points for the motion. We regard (28) as a transformation depending upon the parameter t and wish to calculate its Jacobian $\mathfrak{X}(t,\xi^*)=(x_{i\xi_j})=(x_{i\xi_j}(t,\xi^*))$. This can be done by means of the equation of variation. In fact, taking partial derivatives in (3) gives

$$d(x_{i\xi_j})/dt=\sum X_{ix_r}x_{r\xi_j}. \tag{29}$$

Denoting by $\mathfrak{F}$ the matrix (X_{ix_j}) we see that $\mathfrak{X}$ satisfies the linear differential equation

$$d\mathfrak{X}/dt=\mathfrak{F}\mathfrak{X}, \tag{30}$$

where the initial conditions ξ^* are to be considered as parameters. Setting $\xi=0$ in (30) yields

$$J(T_t)=e^{At}, \tag{31}$$

where A is the matrix of linear terms of (3) at the origin. But then it is clear that condition (I) and (II) for the flow generated by (3) are equivalent to conditions (i_R) and (ii) for the differential equations, while (18) becomes replaced by

$$k>\Lambda/\lambda, \tag{32}$$

where $\Lambda=\max|\operatorname{Re}\lambda_i|$ and $\lambda=\min|\operatorname{Re}\lambda_i|$. We have thus proved

THEOREM 4. *Any system of differential equations* (3) *defined in some neighborhood of the origin such that $X_i(0,\cdot\cdot\cdot,0)=0$, satisfying conditions* (i) *and* (ii) *and of class C^k where k satisfies* (32) *can be linearized by a change of coordinates in T^k.*

For the case of analytic differential equations satisfying the (i) and (ii) we can assert that the change of coordinates is analytic. In this case, by the introduction of a complex time, if necessary, we can reduce (i_R) to (i). We thus obtain

THEOREM 5 (Poincaré). *Any system of analytic differential equations*

(3) *satisfying* (i) *and* (ii) *can be linearized by an analytic change of coordinates.*

8. As was shown in Section 3, if the formal condition (ii) is not satisfied, then a contraction can, in general, not be linearized. We can, nevertheless, ask for some other, nonlinear, normal form. Let us first examine where the proof of Lemma 1 breaks down if (ii) does not hold. In fact, let $s_i = s_1^{m_1} \cdots s_n^{m_n}$ where the m_j are integers such that $\sum m_j > 1$. Then, if we set $(i_1, \cdots, i_n) = (m_1, \cdots, m_n)$ in (17) we obtain $P^i_{m_1 \cdots m_n} = 0$. Since $P^i_{m_1 \cdots m_n}$ is a polynomial in the lower order $r^j_{j_1 \cdots j_n}$ which are already uniquely determined, this might not vanish, so that (16) can not in general be satisfied. We can remedy this situation by including the value of these $P^i_{m_1 \cdots m_n}$ into the normal form itself. More precisely,

LEMMA 5. *Let T be an element of F^∞ whose matrix of linear terms has no multiple elementary divisors, with eigenvalues $s_1, \cdots, s_n$. Let M_i denote the collection of n-tuplets $(m_1, \cdots, m_n)$ of positive integers such that*

$$s_i = s_1^{m_1} \cdots s_n^{m_n}. \tag{33}$$

Then there exists a transformation R in F^∞ such that RTR^{-1} has the (complex) form

$$N = (\cdots, s_i x_i + \sum A^i_{m_1 \cdots m_n} x_1^{m_1} \cdots x_n^{m_n}, \cdots), \tag{34}$$

where the $(m_1, \cdots, m_n)$ are in M^i.

The equation corresponding to (16) is

$$\begin{aligned} & s_i[x_i + \sum r^i_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}] + \sum_{M_i} A^i_{m_1 \cdots m_n} [x_1 + \sum r^1_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}]^{m_1} \\ & \qquad + \cdots [x_n + \sum r^n_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}]^{m_n} \\ & = s_i x_i + \sum r^i_{i_1 \cdots i_n} (s_1 x_1)^{i_1} \cdots (s_n x_n)^{i_n} + \cdots . \end{aligned} \tag{35}$$

If we compare the coefficients of $x_1^{i_1} \cdots x_n^{i_n}$ for $(i_1, \cdots, i_n)$ not in M^i we obtain (17) where the $P^i_{i_1 \cdots i_n}$ is a polynomial in those $r^j_{j_1 \cdots j_n}$ and $A^i_{m_1 \cdots m_n}$ for which $\sum j_k$ and $\sum m_k$ are both $< \sum i_k$. We can then solve (17) for $r^i_{i_1 \cdots i_n}$ in terms of known quantities, as before. If $(i_1 \cdots i_n)$ is in M^i, then (17) is replaced by

$$s_i r^i_{i_1 \cdots i_n} + A^i_{i_1 \cdots i_n} = (s_1^{i_1} \cdots s_n^{i_n}) r^i_{i_1 \cdots i_n} + P^i_{i_1 \cdots i_n}. \tag{36}$$

The coefficients of $r^i_{i_1 \cdots i_n}$ in (36) cancel and we can determine that $A^i_{i_1 \cdots i_n}$. We then can choose the $r^i_{i_1 \cdots i_n}$ arbitrarily and (35) will hold. (If we wish

to make the $A^i{}_{m_1 \cdots m_n}$ unique, we should make some a priori choice of all such $r^i{}_{i_1 \cdots i_n}$, which might arise, e. g., set them all equal to zero.) This proves the lemma.

If we now assume that condition (i) holds, then (ii) can be violated only for those $(m_1, \cdots, m_n)$ such that $\sum m_i < k$ where k is given by (18). Thus, in finding a normal form for arbitrary T satisfying (i) and not (ii) all that is necessary is to show that we can choose coordinates in such a manner that T becomes a transformation given by polynomials of degree k. This can be done by the same method as in the proof of Theorem 2:

THEOREM 6. *Let T be a transformation in T^r where $r \geqq k$ and k satisfies* (18) *where the s_i are the eigenvalues of $J(T)$. Then there is a transformation R in T^r such that*

$$P = RTR^{-1}, \tag{37}$$

where P is a transformation given by polynomials of degree $\leqq k$. In fact we can assume that P is given by the image of T in F^k under the natural homomorphism. We can determine a normal form for T by application of Lemma 5.

Proof. It is easy to see that

$$\| P^{-1}S_1T - P^{-1}S_2T \|^r{}_N < \epsilon \| S_1 - S_2 \|^r{}_N + \| L^{-1}S_1T - L^{-1}S_2T \|^r{}_N \tag{38}$$

for any S_1 and S_2 in T^r. If we take $S_1 = P^{-j-1}RT^{j+1}$ and $S_2 = P^{-j}RT^{-j}$, then $S_1 - S_2$ is an element of $V^r{}_N$ if R is a suitably chosen polynomial transformation (reducing to the identity if $r = k$). Then an application of Lemma 4 implies that the series

$$\sum (P^{-j-1}RT^{j+1} - P^{-j}RT^j) \tag{39}$$

converges, proving the theorem.

In the particular case of an analytic transformation in the plane with real eigenvalues $0 < s < t < 1$ for the Jacobian at the origin, Theorem 6 implies that every such surface transformation can be brought into the normal form

$$\begin{aligned} &x^1 = sx + Ay^m, \quad && y' = ty \ \ (\text{if } s = t^m) \\ \text{or} \quad & && \\ &x^1 = sx \quad , && y' = ty \ \ (\text{if } s \neq t^m \text{ for any } m) \end{aligned} \tag{40}$$

by an analytic change of coordinates; this result was obtained by Lattès [3].

9. In this section we shall consider what happens if (i) is violated. We can not obtain anything approaching a normal form for these transformations, but we shall, nevertheless, outline the proof of a result which is a strong generalization of Theorems 2-6. In what follows, we shall assume for simplicity that all the eignevalues of the Jacobian matrices are real. The transition to the case of non-real eignevalues does not imply any essentially new ideas.

THEOREM 7. *Let T be a transformation in T^k of the form*

$$x^1_i = s_i x_i + g_i(x_1, \cdots, x_n), \tag{41}$$

where the g_i are terms of higher order and

$$|s_i| < 1 \text{ for } i \leqq p, \qquad |s_i| \geqq 1 \text{ for } i > p. \tag{42}$$

Suppose, furthermore that

$$s_j \neq s_1^{m_1} \cdots s_p^{m_p} \qquad (j = 1, 2, \cdots, p) \tag{43}$$

for any positive integers m_i such that $\sum_1^p m_i > 1$, and that k satisfies (18) *where S and s are now defined by*

$$S = \max(|s_1|, \cdots, |s_p|) \text{ and } s = \min(|s_1|, \cdots, |s_p|), \tag{44}$$

Then there exists a change of coordinates R in T^k of the particular form

$$y_i = x_i - \phi(x_1, \cdots, x_p) \tag{45}$$

which transforms T into the form

$$y'_i = s_i y_i + G_i(y_1, \cdots, y_n), \tag{46}$$

where the G_i satisfy

$$G_i(y_1, \cdots, y_p, 0, \cdots, 0) = 0 \tag{47}$$

for all i.

It is clear that Theorem 2 is contained in Theorem 6. (Take $p = n$.) If we do not assume (43) we have

THEOREM 8. *Let T be a transformation in T^k of the form* (41) *satisfying* (42) *and* (18). *Then there exists a change of coordinates R in T^k of the form* (45) *transforming T into the form* (47) *where $G_i(y_1, \cdots, y_p, 0, \cdots, 0)$ is a polynomial of degree $[\log s/\log S] + 1$ for $i \leqq p$ and*

$$G_i(y_1, \cdots, y_p, 0, \cdots, 0) = 0 \text{ for } i > p. \tag{48}$$

It is clear that Theorem 7 follows from Theorem 8 via Lemma 1 so that it suffices to prove Theorem 8. It should be remarked that Theorem 8 implies that the surface $y_{p+1} = \cdots y_n = 0$ remains invariant. A more general formulation of this result which does not make use of the somewhat restrictive smoothness assumption (18) and (44) is contained in

THEOREM 9. *Let T be a transformation in T^k of the form* (41) *where the S_i satisfy* (42). *Then there exists a change of coordinates R in T^k of the form*

$$(49) \qquad y_i = x_i, \quad (i \leqq p); \qquad y_i = x_i - \phi_i(x_1, \cdots, x_p) \quad (i > p)$$

which transforms T into the form (46) *where the G_i satisfy* (48).

If we apply Theorem 6 to the invariant surface $y_{p+1} = \cdots y_n = 0$ (assuming that T satisfies the additional smoothness assumption (44)) then Theorem 8 follows from Theorem 9. If q of the eigenvalues s_i are greater than one then applying Theorem 9 to T^{-1} we obtain

THEOREM 10. *Let T be a transformation in T^k of the form* (41) *where p of the s_i are < 1 and q of the s_i are > 1. Then there exist invariant surfaces of class C^k passing through the origin of dimensions $n - p$ and $n - q$.*

Theorem 10 is a complete generaliaztion (to n-dimensions and the non-analytic case) of the result of Poincaré concerning the existence of invariant curves near a hyperbolic point of a surface transformation, cf. [6], pp. 202-204, [2] and [8]. In the case of surface transformations $n = 2$, $p = q = 1$.

If we make use of a slight modification of Lemma 4 and of the remarks before Theorem 5 we can translate Theorem 7 into a theorem about differential equations.

THEOREM 11. *Consider a system of differential equations of the form*

$$(50) \qquad dx_i/dt = \lambda_i x_i + g_i(x_1, \cdots, x_n),$$

where the λ_i satisfy

$$(51) \qquad \lambda_i < 0 \text{ for } i \leqq p,$$

and the g_i are of class C^k where

$$(52) \qquad k > \max_{i \leqq p} |\lambda_i| / \min_{i \leqq p} |\lambda_i|.$$

Then there exists a change of coordinates of the form (45) *transforming* (50) *into the form*

$$(53) \qquad dy_i/dt = \lambda_i y_i + G_i(x_1, \cdots, x_n),$$

where the G_i satisfy (48).

This is a generalization to the non-analytic case of a theorem of Liapounoff [4]. If we similarly translate Theorems 9 and 10 into theorems about differential equations we obtain the 'Asymptotische Bahnen' of Siegel [7] (without his analyticity assumptions).

We have seen that all the results of this section hinge upon Theorem 9. We now proceed to its proof.

Denote by E the projection

$$E:(x_1,\cdots,x_n)\rightarrow(x_1,\cdots,x_p,0,\cdots,0). \tag{54}$$

Then we rephrase the conclusion of Theorem 9 as follows: there exists an R in T^k of the form (49) such that

$$(RTR^{-1})ER=E(RTR^{-1})ER. \tag{55}$$

We first remark that any transformation R of type (49) is uniquely determined by RE. Furthermore, if a sequence R_n of transformaticn of the type (49) has the property that R_nE_n converges uniformly along with partial derivatives of a certain order then the sequence R_n has this same property. Finally R^{-1} has the same form as R with the exception that the ϕ_i are replaced by $-\phi_i$. If we translate equation (55) into a functional equation for the ϕ_i we obtain

$$\begin{aligned} (56)\quad & s_i\phi_i+g_i[x_1,\cdots,x_p,\phi_{p+1}(x_1,\cdots,x_p)\cdots\phi_n(x_1,\cdots,x_p)] \\ &=\phi_i(s_ix_1+g_1[x_1,\cdots,x_p,\phi_{p+1}(x_1,\cdots,x_p),\cdots], \\ &\quad\cdots s_px_p+g_p[x_1,\cdots,x_p,\phi_{p+1}(x_1,\cdots,x_p),\cdots]) \end{aligned}$$

for $i=p+1,\cdots,n$. We write this equation as

$$\begin{aligned} (57)\quad \phi_i=s_i^{-1}\{&\phi_i(s_1x_1+g_1[x_1,\cdots,x_p,\phi_{p+1},\cdots,\phi_n], \\ &\cdots s_px_p+g_p[x_1,\cdots,x_p,\phi_{p+1}(x_1,\cdots,x_p),\cdots]) \\ &-g_i[x_1,\cdots,x_p,\phi_{p+1},\cdots,\phi_n]\}. \end{aligned}$$

We now observe that all the s_j occurring inside the functions in (57) are strictly less than one, while the s_i^{-1} occurring as factors are less than or equal to one as a consequence of (42) and (49). Furthermore the g's occurring in (57) are functions of second order. Applying Taylor's theorem twice, we can, therefore, solve (57) by an iteratuve procedure similar to that used in the proofs of Theorems 2 and 6.

NEW YORK UNIVERSITY.

REFERENCES.

[1] G. D. Birkhoff, *Dynamical Systems*, American Mathematical Society Colloquium Publication, Number 9.

[2] J. Hadamard, *Selecta*, 1901, pp. 163-166.

[3] S. Lattès, *Comptes Rendus*, vol. 152 (1911), pp. 1566-1569.

[4] A. Liapounoff, *Problème générale de la stabilité du mouvement*, Annals of Mathematics Studies, Number 17.

[5] E. Picard, *Traité d'Analyse*, vol. 3.

[6] H. Poincaré, *Oeuvres*, vol. 1.

[7] C. L. Siegel, "Der Dreierstoss," *Annals of Mathematics*, vol. 42 (1941), pp. 156-162.

[8] S. Sternberg, "On the behaviour of invariant curves near a hyperbolic point of a surface transformation," *American Journal of Mathematics*, vol. 75 (1955), pp. 526-534.

[9] S. Sternberg, "On local C^n contractions of the real line," *Duke Mathematical Journal*, vol. 24 (1957), pp. 97-102.

[10] S. Sternberg and P. Ungar, "On a class of functional equations," to appear.

COVERINGS OF ALGEBRAIC CURVES.*

By Shreeram Abhyankar.

1. Introduction. In this paper we present, among other things, some new results concerning coverings of algebraic curves—i. e., in global ramification theory—which distinguish the modular case from the classical, i. e., the characteristic zero case, and seems to open up new lines of research. Throughout the paper several problems will be formulated and questions raised.

We had noted in [A1] that the possibility of "local splitting of a simple branch variety by itself" is the basic fact underlying the difference between local ramification theory in the modular and the classical cases. One thesis of this paper is that the corresponding global possibility of the "splitting of a single branch point by itself" is the basic fact which distinguishes the global ramification theory in the modular case from that in the classical case. For instance, the following three are some of the consequences of this *possibilty*; let the ground field k be algebraically closed of characteristic $p \neq 0$: (1) Given any one-dimensional algebraic function field K/k there exists x in K (not in k) such that $x = \infty$ is the only valuation of $k(x)/k$ ramified in K, i. e., the total differential dx has no zero or pole at finite distance (Theorem 4 of Section 2). [Hasse and Deuring had proved that for each $p \neq 2$ there exist finite number of elliptic function fields of this type.] (2) There exist unsolvable unramified coverings of the affine line—which is a commutative group variety (Section 4). (3) For nontamely ramified extensions, in no possible sense is the monodromy group generated by loops around the branch points (Remark 7 of Section 4). (1) leads to the concept of universal branch loci and the possibility of new invariants. (2) is only a very special consequence of a general pattern which leads us to formulate a conjecture which roughly says that: (ramification theory in characteristic $p \neq 0$) $=$ (ramification theory in characteristic zero for the *corresponding* situation) $+$ (the class of all quasi p-groups[1]); for the local theory some evidence for this conjecture is in our previous papers [A1] and [A3] and some evidence for the global theory for curves is given in this

* Received February 8, 1957.

[1] As defined in [A3], for a given prime number p, a finite group G is said to be a quasi p-group if G is generated by its p-sylow subgroups.

paper (Section 4). This conjecture consists mainly of two parts: the first part asks us to algebraize the fundamental group in the classical case and carry it over to tamely ramified extensions, for this and other comparative purposes we have collected in Section 7 information on the topological fundamental and monodromy groups in the classical case for curves; the second part of the conjecture says that if (for characteristic $p \neq 0$) in a situation, nontrivial coverings are possible, then coverings exist with any assigned quasi p-group.

The recent result of Lang-Serre to the effect that for a curve there are only a finite number of unramified coverings of a given degree is generalized in Section 6 to tamely ramified extensions with assigned branch points. In Section 5 is given a formula to derive from the different of an extension the different of the corresponding least galois extension. In the Appendix (Section 8) are collected some lemmas used in the paper. The contents of the other sections should be clear from their titles; the reader who wants a quick look at the amusing results is referred to Section 4.

Notations. All through the paper we shall tacitly use the notations and results of [A1] and Section 2 of [A2]. Now let t be a power series in $X, Y, \cdots$ with $X = (X_1, X_2, \cdots, X_a)$, $Y = (Y_1, Y_2, \cdots, Y_b) \cdots$ having coefficients in a field k; we shall use the following notations:

$$| t |_X = \text{leading degree of } t \text{ in } X;$$

$$| t |_{X,Y} = \text{leading degree of } t \text{ in } X \text{ and } Y; \text{ etc.}$$

If t is a polynomial in X (in X and Y; etc.) then:

$$\| t \|_X = \text{the degree of } t \text{ in } X;$$

$$\| t \|_{X,Y} = \text{the degree of } t \text{ in } X \text{ and } Y; \text{ etc.}$$

When the reference to X (or X, Y) is clear from the context, we may omit these subscripts. Note that: $| 0 | = \infty$ and $\| 0 \| = -\infty$. For a polynomial $F(Z)$ we shall denote by $DF(Z)$ the Z-discriminant of $F(Z)$.

Now let K/k be an n-dimensional algebraic function field and let K^* be a finite separable extension of K. Let V be a normal projective model of K/k, let V^* be a K^*-normalization of V. Let W be an irreducible subvariety of V and let $W^*_1, \cdots, W^*_s$ be the irreducible subvarieties of V^* corresponding to W; let R and R^*_i be the quotient rings of W and W^*_i on V and V^* respectively; let w be a real discrete valuation of K and let $w^*_1, \cdots, w^*_t$ be the K^*-extension of w. We shall say that respectively $W^*_1/W, R^*_1/R, w^*_1/w$ are *tamely ramified* if in case $p \neq 0$ we have $r(W^*_1 : W)$,

$r(R_1:R)$, $r(w^*_1:w)\not\equiv 0 \pmod p$ respectively. We shall say that respectively W, R, w are *tamely ramified in* K^* if respectively W^*_i/W, R^*_i/R, w^*_i/w are tamely ramified for all i. We shall say that V is tamely ramified in K^* (and K^* or V^* is tamely ramified over V) if each irreducible subvariety of W is tamely ramified in K^*. Observe that for $n=1$, V^* is tamely ramified over V if and only if each valuation of K/k is tamely ramified in K^*; in this case we shall say that K^*/K (or K in K^*) is tamely ramified.

2. Splitting of a single branch point by itself. Let k be an arbitrary field of characteristic $p\neq 0$. In [A1, Remark in Section 2] we had noted that the possibility of "local splitting of a simple branch variety by itself" is the basic fact underlying the difference between the structures of local galois groups in the case of nonzero characteristic and in the case of zero characteristic. This possibility was exhibited by the normal surface S^* [Example 5 of A1]: $Z^{p+1}+Y^{p-1}+X^{p+1}=0$, for the Z-projection of S^* onto the X,Y plane S the branch locus is $D:X=0$. Now we shall exploit this surface, or rather its section by the plane $Y=X$, for global ramification theory and the corersponding conclusion will be that the possibility of "global splitting of a (single) branch point by itself" is the basic fact underlying the difference between the global ramification theories in the case of nonzero characteristic and in the case of zero characteristic.

So consider the polynomial

$$F(Z)=Z^{p+1}+x^{p-1}+x^{p+1}\in k[x][Z],$$

where x is a transcendental over k. Let $Z=Z^*x^2$ and $F^*(Z^*)=x^{-p-1}F(Z)$, so that

$$\begin{aligned}F^*(Z^*)&=x^{-p-1}[(x^2Z^*)^{p+1}+x^{p-1}(x^2Z^*)+x^{p+1}]\\&=x^{p+1}Z^{*p+1}+Z^*+1\equiv 1(Z^*+1)\ [\operatorname{mod} x].\end{aligned}$$

Hence by Hensel's lemma [for instance Lemma 1 on page 43 of C]: $F^*(Z^*)=G^*(Z^*)(Z^*+u)$ where $u\in k[[x]]$ with $u(0)=1$ and $G^*(Z^*)$ is of degree p in Z^* with $G^*(Z^*)\equiv 1\ [\operatorname{mod} x]$. Therefore

$$F(Z)=G(Z)(Z+ux^2),$$

where

$$G(Z)=Z^p+G_1Z^{p-1}+G_2Z^{p-2}+\cdots+G_p,\qquad G_i\in k[[x]].$$

Then

$$\begin{aligned}F(Z)=Z^{p+1}&+(G_1+ux^2)Z^p+(G_2+ux^2G_1)Z^{p-1}+\cdots\\&+(G_{i+1}+ux^2G_i)Z^{p-i}+\cdots+(G_p+ux^2G_{p-1})Z+ux^2G_p.\end{aligned}$$

Hence

(1) $$G_1 + ux^2 = G_2 + ux^2G_1 = \cdots = G_{p-1} + ux^2G_{p-2} = 0$$

(2) $$G_p + ux^2G_{p-1} = x^{p-1}$$

and

(3) $$ux^2G_p = x^{p+1}.$$

Now (1) implies that

$$G_1 = -ux^2, \quad G_2 = -ux^2G_1, \quad G_3 = -ux^2G_2, \cdots, G_p = -ux^2G_{p-2},$$

so that

(4) $$G_1 = -ux^2, \quad G_2 = u^2x^4, \quad G_3 = -u^3x^6, \cdots, G_i = (-1)^i u^i x^{2i}, \cdots, G_{p-1} = (-1)^{p-1}u^{p-1}x^{2(p-1)},$$

i. e., $G_{p-1} = u^{p-1}x^{2p-2}$. Hence by (2) we have

(5) $$G_p = x^{p-1} - ux^2G_{p-1} = x^{p-1} - u^px^{2p} = x^{p-1}(1 - u^px^{p+1}).$$

Since $u(0) = 1$, $|u| = 0$. Hence by (4) and (5) we have:

(6) $$|G_i| = 2i \text{ for } i = 1, 2, \cdots, p-1 \text{ and } |G_p| = p-1.$$

Therefore by Lemma A1 (of Section 8) $G(Z)$ is irreducible in $k[[x]][Z]$. Let v be the valuation of $k((x))/k$ given by x, let z be a root of $G(Z)$, w be the unique extension of v to $k((x))(z)$. Then [O, Theorem II on page 298] $w(z) = (1/p)w(G_{p-1}) = [(p-1)/p]w(x)$. Therefore $\bar{r}(w:v)$ is divisible by p and hence $\bar{r}(w:v) = p$ and (the residue field of w) = (the residue field of v) = k. Thus

(7) $$F(Z) = G(Z)(X + ux^2), \ G(Z) \text{ irreducible in } k[[x]][Z].$$

Hence if $F(Z)$ were reducible in $k[x][Z]$ it must have $Z + u^*$ as a factor with $u^* = ux^2 \in k[x]$. Then

$$0 = F(-u^*) = u^{*p+1} - x^{p-1}u^* + x^{p+1}.$$

Hence the x-degrees of two of the three terms u^{*p+1}, $x^{p-1}u^*$, x^{p+1} must be equal. Now $\| u^{*p+1} \| \geqq | u^{*p+1} | = 2(p+1) > p+1 = \| x^{p+1} \|$; and $\| u^{*p+1} \| = \| x^{p-1}u^* \|$ implies $\| u^{*p} \| = \| x^{p-1} \| = p-1$, i. e., $\| u^* \| = (p-1)/p =$ a noninteger which is a contradiction. Therefore $\| x^{p-1}u^* \| = \| x^{p+1} \|$, i. e., $\| u^* \| = 2$. Since $| u^* | = 2$ we must have $u^* = cx^2$ with $0 \neq c \in k$. Now $F(-cx^2) = c^{p+1}x^{2p+2} - cx^{p+1} + x^{p+1}$ so that $\| F(-cx^2) \| = 2p+2$ which is a contradiction since $F(-cx^2) = 0$.

Thus $F(Z)$ is irreducible in $k[x][Z]$ and hence in $k(x)[Z]$ and $F(Z)$

factors in $k[[x]][Z]$ i. e., in $k((x))[Z]$ into two irreducible factors of degrees p and 1 respectively and these factors do not introduce any residue field extensions.

[*Remark* 1. It would be interesting to compute the galois group of $F(Z)$ over $k((x))$, i. e., (assuming k to be algebraically closed) by Lemma A2 (of Section 8) the galois group of $Z^p + x^2Z^{p-1} + x^{p-1}$ over $k((x))$; that ought to yield the galois group of $F(Z)$ over $k(x)$.]

Let $K = k(x)$, let z be a root of $F(Z)$ and let $K^* = K(z)$. Let C be the irreducible curve: $Z^{p+1} + X^{p-1}Z + X^{p+1} = 0$ in the X, Z plane and let L be the X axis. Then $K = k(L)$, $K^* = k(C)$ and the rational map given by the embedding $K \subset K^*$ corresponds to the projection of C (by lines parallel to the Z-axis) onto L. Now $F'(Z) = Z^p + x^{p-1}$ so that $F(Z) = ZF'(Z) + x^{p+1}$ and hence $DF(Z) = x^{p(p+1)}$. Therefore the origin, i. e., the valuation v given by the irreducible nonunit x of $k[x]$, is the only possible branch point on L at finite distance. To test for the point at infinity let $x_1 = 1/x$, $Z_1 = Zx_1$ and $F_1(Z_1) = x_1^{p+1}F(Z)$ so that

$$F_1(Z_1) = x_1^{p+1}(x_1^{-p-1}Z_1^{p+1} + x_1^{-p+1}x_1^{-1}Z_1 + x_1^{-p-1}) = Z_1^{p+1} + x_1Z_1 + 1.$$

Now $F'_1(Z_1) = Z_1^p + x_1$ so that $F_1(Z_1) = Z_1F'_1 + 1$ and hence $DF_1(Z_1) = 1$. Therefore the point at infinity is not ramified. Thus the origin of L is the only possible branch point. From the way $F(Z)$ factors in $k((x))[Z]$ we conclude that v splits in K^* into two valuations w_1 and w_2 both of which are rational over k with $\bar{r}(w_1 : v) = d(w_1 : w) = p$ and $\bar{r}(w_2 : v) = d(w_2 : v) = 1$. Now the curve C is of degree $p + 1$ and it has a p-fold point at the origin. Therefore C is rational (over k), i. e., there exists y in K^* such that $K^* = k(y)$, since w_1 and w_2 are rational over k we may assume that they correspond to $y = 0$ and $y = \infty$ respectively (Lemma A3 of Section 8).

[If k is algebraically closed and if we were willing to deal with a generic section of S we could *perhaps* argue thus (and in fact this is how we were led to the construction we have just given): Let $L : aX + bY = 0$ $(a, b \in k)$ be a *generic* line in the X, Y plane S; then the curve C on the surface S^* which corresponds to L is irreducible; C is the intersection of S^* with the *plane* $aX + bY = 0$ in the X, Y, Z space; for the induced rational map of C onto L the branch locus $\bar{D}$ is the intersection of L with D, i. e., $\bar{D}$ is a single point and since $[k(C) : k(L)] = p + 1$ it follows by Proposition 6 (Section 3) that $\bar{D}$ splits in $k(C)$ into two points with ramification indices p and 1 respectively.]

To find y explicitly we may proceed as follows. Homogenizing

$Z^{p+1}+X^{p-1}Z+X^{p+1}=0$ we get $Z^{p+1}+X^{p-1}YZ+X^{p+1}=0$. Thus the p-fold singularity of C is: $X=0$, $Y=1$, $Z=0$. Take $X=0$ to be the line at infinity. Let $x'=Y/X$ and $y=Z/X$; previously we had $x=X/Y$ and $z=Z/Y$, i.e., $y=z/x$ and $x'=1/x$, i.e., $z=y/x'$ and $x=1/x'$ so that $(y/x')^{p+1}+(1/x'^{p-1})y+(1/x'^{p+1})=0$, i.e., $y^{p+1}+x'y+1=0$. Hence $1/x=x'=(-1-y^{p+1})/y=-(1/y)-y^{p}$. Now $x=0$ if and only if $x'=\infty$. Replace x by $(-x')$. Then $y^{p+1}-xy+1=0$, so that $x=y^{p}+y^{-1}$, $x=\infty$ is the only branch point in $k(x)/k$ for $k(y)$ and on it lie $y=0$ and $y=\infty$. If we replace y by y^{-1} then $y^{p+1}-xy^{p}+1=0$, $x=y+y^{-p}$, $x=\infty$ is the only branch point and on it lie $y=0$ and $y=\infty$. Thus we may state and directly reprove

THEOREM 1. *Let $k(y)$ be a simple transcendental extension of an arbitrary ground field k of characteristic $p\neq 0$. Let $x=y+y^{-p}$. Then (1) $[k(y):k(x)]=p+1$; (2) $v\colon x=\infty$ is the only valuation of $k(x)/k$ which is ramified in $k(y)$; (3) v splits in $k(y)$ in the valuations $w_0\colon y=0$ and $w_\infty\colon y=\infty$; and (4) $d(w_0:v)=p$ and $d(w_\infty:v)=1$.*

Proof. $x=y+y^{-p}=(y^{p+1}+1)/y^{p}$; since the numerator and denominator are coprime we have $[k(y):k(x)]=p+1$ and $y^{p+1}+xy^{p}+1=0$ is the minimal equation of y over $k(x)$ [see § 63 of V] i.e., $F(X)=Z^{p+1}+xZ^{p}+1$ is the minimal monic polynomial of y over $k(x)$. Now $F'(Z)=Z^{p}$ so that $DF(Z)=1$ and hence no valuation of $k(x)/k$ except possibly v is ramified in $k(y)$. Also the equation $x=y+y^{-p}$ implies that if w is a valuation of $k(y)/k$ with $w\neq w_0$ and $w\neq w_\infty$ then $w(x)\geqq\min[w(y),w(y^{-p})]=0$ and hence w_0 and w_∞ are the only valuations of $k(y)/k$ which can possibly lie over v. Since $1/x=y^{p}/(y^{p+1}+1)$, $w_0(1/x)=p$ and hence w_0 does lie over v and $d(w_0:v)=\bar{r}(w_0:v)=p$. Again

$$(1/x)=y^{p}/(y^{p+1}+1)=[y^{-p-1}y^{p}]/[y^{-p-1}(y^{p+1}+1)]=y^{-1}/(1+y^{-p-1})$$

so that $w_\infty(1/x)=w_\infty(y^{-1})-w_\infty(1+y^{-p-1})=1$ and hence w_∞ does lie over v and $d(w_\infty:v)=\bar{r}(w_\infty:v)=1$. [Check:

$$p+1=[k(y):k(x)]=\textstyle\sum_{w\text{ over }v}d(w:v)=d(w_0:v)+d(w_\infty:v)=p+1.]$$

THEOREM 2. *Let $k(y)$ be a simple transcendental extension of an arbitrary ground field k of characteristic $p\neq 0$. Let $w_1,w_2,\cdots,w_n$ be a finite set of given valuations of $k(y)/k$ which are rational over k, i.e., we are given a finite set of distinct elements $c_1,c_2,\cdots,c_n$ in $k\cup\{\infty\}$ such that c_i is the residue of y at w_i. Then there exists x in $k(y)$ (not in k) such that $v\colon x=\infty$ is the only valuation of $k(x)/k$ which is ramified in $k(y)$ and $w_1,w_2,\cdots,w_n$ lie above v.*

Proof. It is enough to prove that there exists a subfield K of $k(y)$ such that K is a simple transcendental extension of k such that $w_1, w_2, \cdots, w_n$ contract in K to a single caluation v and v is the only valuation of K/k ramified in $k(y)$; for then the rationality of w_1/k implies the rationality of v/k and by Lemma A3 of Section 8 we may find a generator x of K/k such that v corresponds to $x=\infty$. Now we shall make induction on n: for $n=1$, we may take $K=k(y)$, so let $n>1$ and assume the theorem for $n-1$. Then by the induction hypothesis there exists a simple transcendental extension L of k contained in $k(y)$ such that $w_1, w_2, \cdots, w_{n-1}$ contract in L to a single valuation u_0 and u_0 is the only valuation of L ramified in $k(y)$. Let u_∞ be the contraction of w_n to L. If $u_0 = u_\infty$ we may take $K=L$, so now assume that $u_0 \neq u_\infty$. By Lemma A3 of Section 8 we can find a generator y' of L/k such that u_0 is $y'=0$ and u_∞ is $y'=\infty$. Applying Theorem 1 to $k(y')/k$ find x in L (not in k) such that $v\colon x=\infty$ is the only valuation of $k(x)/k$ which is ramified in L and u_0 and u_∞ are exactly the valuations of L lying above v. If we let $K=k(x)$ the induction is complete.

Remark 2. If k is finite, we may take $w_1, w_2, \cdots, w_n$ to be all the rational valuations of $k(y)/k$. Then all the rational points of the y-line will lie on the point at infinity of the x-line so that each finite rational point of the x-line will undergo residue field extensions but no ramification. *Question. How far can we assign these residue field extensions?*

PROPOSITION 1. *Let $k(y)$, w_0 and w_∞ be as in Theorem* 1. *If we take $x=y^t+c_1y^{-p}+c_2y^{-2p}+\cdots+c_hy^{-hp}$ with $c_1, c_2, \cdots, c_h$ in k, $c_h \neq 0$, $t>0$ with $t \not\equiv 0 \pmod p$, then* (1) $[k(y):k(x)]=hp+t$; (2) *$v\colon x=\infty$ is the only valuation of $k(x)/k$ which is ramified in $k(y)$; v splits in $k(y)$ into w_0 and w_∞; and* (4) *$d(w_0:v)=hp$ and $d(w_\infty:v)=t$.*

Proof. This is similar to the proof of Theorem 1.

PROPOSITION 2. *Let $k(y)$ and $w=w_\infty$ be as in Theorem* 1. *If we take $x=c_0y+c_1y^p+\cdots+c_{m-1}y^{(m-1)p}+y^{mp}$ with $c_0, c_1, \cdots, c_{m-1}$ in k and $c_0 \neq 0$ then* (1) $[k(y):k(x)]=mp$; (2) *$v\colon x=\infty$ is the only valuation of $k(x)/k$ which is ramified in $k(y)$; and* (3) *w is the only valuation of $k(y)$ lying above v [so that $d(w:v)=\bar{r}(w:v)=mp$].*

Proof. Now $F(Z)=Z^{mp}+c_{m-1}Z^{(m-1)p}+\cdots+c_1Z^p+c_0Z-x$ is the minimal monic polynomial of y over $k(x)$; $F'(Z)=c_0$ and hence $DF(Z)=c_0{}^{mp}$ so that $v\colon x=\infty$ is the only valuation of $k(x)/k$ which can possibly be ramified in $k(y)$. Let w^* be a valuation of $k(y)/k$. Then from the equation

defining x it is clear that $w^*(y) \geqq 0$ if and only if $w^*(x) \geqq 0$ and hence $w: y = \infty$ is the only valuation of $k(y)$ lying above $v: x = \infty$.

We may strengthen Theorem 2 thus:

THEOREM 3. *Let the notation be as in Theorem 2. By Lemma* A3 *of Section* 8 *we may assume that* $c_1 = \infty$. *Assume* $n > 1$ *and let* $m_2, m_3, \cdots, m_n$ *be arbitrary positive integers which are divisible by* p *and let* $m_1 = 1$. *Let* $x = y + (y - c_2)^{-m_2}(y - c_3)^{-m_3} \cdots (y - c_n)^{-m_n}$. *Then* (1) $[k(y):k(x)] = m_1 + m_2 + \cdots + m_n$; (2) $v: x = \infty$ *is the only valuation of* $k(x)/k$ *which is ramified in* $k(y)$; (3) $w_1, w_2, \cdots, w_n$ *are exactly the valuations of* $k(y)$ *which lie above* v; *and* (4) $d(w_i : v) = \bar{r}(w_i : v) = m_i$ *for* $i = 1, 2, \cdots, n$.

Proof. This is similar to the proof of Theorem 1.

Remark 3. In reference to Theorem 3, by Proposition 6 (Section 3) we know that at least one of the m_i is divisible by p. However, in Theorem 3 we have assumed that $m_1 = 1$ and the other m_i are divisible by p; invoking Proposition 2 before applying Theorem 3, we may take m_1 also to be an arbitrary integer divisible by p. *Question. How far can the assumptions on the* m_i *be relaxed?*

Given $w_1, \cdots, w_n$ and $m_1, \cdots, m_n$ determine all x—or rather $k(x)$—of the type described in Theorem 3 or rather determine all possible structures of $k(y)/k(x)$. Now reverse the problem: i. e., suppose $k(x)$, v and $m_1, \cdots, m_n$ are given. Find all finite algebraic extensions K^* of $K = k(x)$ [to begin with those K^* which are simple transcendental extensions of k and then others as well] such that v is the only valuation of $k(x)/k$ which is ramified in K^*, there are n valuations $w_1, \cdots, w_n$ of K^*/k lying above v and $d(w_i : v) = m_i$ for $i = 1, \cdots, n$. Do this for k algebraically closed and $n = 1$, then $n = 2$ and so on. Is there any smallest value of n which would yield all function fields? Now replace $k(x)$ by an arbitrary one-dimensional function field.

From Theorem 2, we at once derive the following theorem which will be put into its right perspective in Section 4.

THEOREM 4. *Let* K *be a simple transcendental extension of an algebraically closed field* k *of characteristic* $p \neq 0$ *and let* v *be a valuation of* K/k. *Then* (I) *given a one-dimensional algebraic function field* L/k *there exists a finite algebraic extension* L_1 *of* K *such that* L_1 *is* k*-isomorphic to* L *and such that* v *is the only valuation of* K/k *which is possibly ramified in* L. *Also* (II) *given a one-dimensional algebraic function field* L/k *and a finite separable algebraic extension* L^* *of* L *there exists a finite algebraic*

extension L_1 of K and a finite algebraic extension L^*_1 of L_1 such that L^*_1 is isomorphic to L^* under a k-isomorphism which maps L_1 onto L and v is the only valuation of K/k which is possibly ramified in L^*_1.

Proof. Taking $L = L^*$, (I) follows from (II), hence it is enough to prove (II). Fix y in L, not in k, and let $K^* = k(y)$. Let $w_1, w_2, \cdots, w_n$ be the valuations of K^*/k which are ramified in L^* (if no valuation of K^*/k is ramified in L^* we may take for $w_1, \cdots, w_n$ any valuations of K^*/k). By Theorem 2 there exists x in K^*, not in k, such that $w_1, \cdots, w_n$ contact in $k(x)$ to a single valuation w and w is the only valuation of $k(x)/k$ which is ramified in K^*. By Lemma A3 of Section 8 there exists a k-isomorphism s of $k(x)$ onto K which maps w onto v; extend s to an isomorphism t of L^* into an algebraic closure of K, let $L^*_1 = t(L^*)$ and $L_1 = t(L)$. Then v is the only valuation of K/k which is possibly ramified in L^*_1.

Remark 4. Part (I) of Theorem 4 may also be stated thus: "Given a one-dimensional algebraic function field L over an algebraically closed ground field k of characteristic $p \neq 0$, there exists x in L not in k such that $x = \infty$ is the only valuation of $k(x)/k$ ramified in L; in other words, the total differential dx has no zeros or poles except at $x = \infty$." An extremely special case of this is known, namely it follows from the work of Hasse [H] and Deuring [D], see also Serre [S], that for each value of $p \neq 2$, there exist a finite number of elliptic function fields L/k for which this is true; of course we prove it for *all* function fields.

3. Coverings of the line with one, two or three branch points.

In this section, K denotes a simple transcendental extension of an algebraically closed field k of characteristic p, and S_n denotes the symmetric group on n letters.

PROPOSITION 3. *Let v_1, v_2, v_3 be any three distinct valuations of K/k and let n be a positive integer bigger than one such that either* (I) *n, $n-1 \not\equiv 0 \pmod p$ in case $p \neq 0$, or* (II) *n is odd and n, $n-2$, $2 \not\equiv 0 \pmod p$ in case $p \neq 0$. Then there exists a finite algebraic extension L/K such that* (1) *L/k is a simple transcendental extension,* (2) *for a least normal extension L^* of K containing L, the galois group of L^*/K is isomorphic to S_n,* (3) *v_1, v_2, v_3 are exactly the valuations of K which are ramified in L, i.e., in L^* (except when $n = 2$ in which case only v_1 and v_2 are ramified), and* (4) *K is tamely ramified in L and hence (by Proposition 7 of Section 5) in L^*.*

Proof. Let $L = k(y)$ be a simple transcendental extension of k,

let $x = y^{n-1}(y-1)$ and $f(Z) = Z^{n-1}(Z-1) - x$ in case (I) and let $x = y^{n-2}(y-1)^2$ and $f(Z) = Z^{n-2}(Z-1)^2 - x$ in case (II). Then $[L:k(x)] = n$ and $f(Z)$ is the minimal monic polynomial of y over $k(x)$ [§ 63 of V], and in view of Lemma A3 of Section 8 it is enough to prove that there are exactly three valuations of $k(x)/k$ which are ramified in L and $f(Z)$ is unaffected over $k(x)$, i.e., the galois group of $f(Z)$ over $k(x)$ is S_n. Let w_0, w_1, w_∞ be the valuations of $k(y)/k$ given by $y = 0, 1, \infty$ respectively and let v_0, v_∞ be the valuations of $k(x)/k$ given by $x = 0, \infty$ respectively. It is clear from defining equations of x that $w_\infty(x) = -n$ so that w_∞ lies above v_∞ and $d(w_\infty : v_\infty) = n$ so that w_∞ is the only valuation of $k(y)$ lying above v_∞; also in case (I): $w_0(x) = n-1$, $w_1(x) = 1$, $n - 1 + 1 = n = [k(y):k(x)]$ and in case (II): $w_0(x) = n-2$, $w_1(x) = 2$, $n - 2 + 2 = n = [k(y):k(x)]$, hence in either case w_0 and w_1 are the only valuations of $k(y)$ lying above v_0. Now $(n-1) + [(n-1) - 1] = 2n - 3 = (n-1) + [(n-2) - 1] + [2 - 1]$ and hence in either case $2n-3$ is the contribution of v_0 and v_∞ to the degree λ of the different of $k(y)$ over $k(x)$. Since both these fields are of genus zero, we have: $-2 = \lambda - 2n$, i.e., $\lambda = 2n - 2$ so that $\lambda - (2n-3) = 1$. Hence there is only one more valuation v of $k(x)$ which is ramified in $k(y)$ and only one valuation w of $k(y)$ lying above v is ramified over v and $d(w:v) = 1 + 1 = 2$ [v will be different in cases I and II; its value can at once be found, by computing $Df(Z)$, to be $x = -n^{-n}(n-1)^{n-1}$ and $x = 4n^{-n}(n-2)^{n-2}$ respectively]. Since $p \neq 2$, $2 \not\equiv 0 \pmod{p}$ and hence it follows [by Section 5 and Lemma A5 of Section 8] that if t is a uniformizing parameter at v then the galois group of $f(Z)$ over $k((t))$ is generated by a 2-cycle and hence the galois group of $f(Z)$ over $k(x)$ contains a 2-cycle. In case (I) the galois group of $f(Z)$ over $k((x))$ is generated by an $(n-1)$-cycle [see Section 5 and Lemma A5 of Section 8] and hence the galois group of $f(Z)$ over $k(x)$ contains an $(n-1)$-cycle and hence it must be S_n [Lemma 1 of A3]. Again in case (II) the galois groups of $f(Z)$ over $k((x))$ and $k((1/x))$ are generated respectively by an n-cycle and by a permutation of type $(1,2)(3,4,\cdots,n)$ so that the galois group of $f(Z)$ over $k(x)$ contains an n-cycle and a permutation of type $(1,2)(3,4,\cdots,n)$ and hence it must be S_n [Lemma 3 of A3].

Proposition 4. *Assume that $p \neq 2$. Let v_1, v_2, v_3 be any three distinct valuations of K/k and let q be any integer. Then there exists a tamely ramified finite algebraic extension L of K such that* (I) *L/k is simply transcendental,* (II) *v_1, v_2, v_3 are exactly the valuations of K/k which are*

ramified in L and (III) (*the number of valuations of L lying above v_1, v_2, v_3*) $\geqq q+1$.

Proof. By any one of the constructions used in the proof of Proposition 3, there exists a finite algebraic extension K_1 of K such that (I.1) K_1/k is simple transcendental, (II.1) v_1, v_2, v_3 are exactly the valuations of K/k which are ramified in K_1 and (III.1) if by q_1 we denote the number of valuations of K_1 lying above v_1, v_2, v_3 then $q_1 \geqq 3+1$. Replacing K and v_1, v_2, v_3 by K_1 and any three valuations of K_1/k lying above v_1, v_2, v_3 obtain K_2; then from K_2, obtain K_3 and so on; denote by q_n the number of valuations of K_n lying above v_1, v_2, v_3. Then $q_n \geqq 3+n$ and hence it is enough to take $L=K_q$.

PROPOSITION 5. *Assume $p=2$, let n be any positive integer and let v_1 and v_2 be any two valuations of K/k. Then there exists a galois extension L of K with galois group isomorphic to S_n such that v_1 and v_2 are the only valuations of K/k which are possibly ramified in L.*

Proof. For $n=1$ or 2 the matter being trivial we assume $n>2$. If n is even, let $F(Z)=Z^n+f_1Z^{n-1}+f_2Z^{n-2}+\cdots+f_{n-2}Z^2+(f_{n-1}+y)Z+f_n$ be any one of the polynomials obtained in Chapter I of [A3]; we may replace $f_{n-1}+y$ by y so that $F(Z)=Z^n+f_1Z^{n-1}+\cdots+f_{n-2}Z^2+yZ+f_n$ and $DF(Z)=y^n$. If n is odd, let $F(Z)=Z^n+f_1Z^{n-1}+f_2Z^{n-1}+\cdots+f_{n-1}Z+f_n+y$ be any one of the polynomials obtained in Chauter II of [A3]; we may replace f_n+y by y so that $F(Z)=Z^n+f_1Z^{n-1}+f_2Z^{n-2}+\cdots+f_{n-1}Z+y$ and $DF(Z)=y^{n-1}$. Thus in either case we have

$$F(Z)=Z^n+F_1Z^{n-1}+F_2Z^{n-2}+\cdots+F_n,$$

with $F_i\in k[x,y]$ and $DF(Z)=y^n$ or y^{n-1} according as n is even or odd. Let S be the projective x, y plane over k so that $k(S)=k(x,y)=K^*$ and let S^* be a normalization of S into a root field L^* of $F(Z)$ over K^*. Then the branch locus of S^* over S is contained in the union Δ of the x-axis $(y=0)$ and the line at infinity in S and by the results of [A3], the galois group of L^*/K^* is isomorphic to S_n. Let S_1 be a *generic* line (rational over k) in S and let S^*_1 be the curve on S^* corresponding to S_1. Then as in [L2], S^*_1 is irreducible, the branch locus of S^*_1 over S is contained in $S_1\cap\Delta$ and hence consists of at most two points and $k(S^*_1)$ is a galois extension of $k(S_1)$ with galois group isomorphic to S_n. Since $k(S_1)/k$ is simply transcendental, we are through by invoking Lemma A3 of Section 8.

PROPOSITION 6. *Let L be a finite algebraic extension of K with* $[L:K]$

$= m > 1$. *Then* (I) *there is at least one valuation of* K/k *which is ramified in* L. (II) *If there is only one valuation of* K *which is ramified in* L, *then it must be nontamely ramified.* (III) *If* L/K *is tamely ramified and if there are only two valuations of* K/k *which are tamely ramified in* L, *then* L/K *is cyclic and* $m \not\equiv 0 \pmod{p}$ *in case* $p \neq 0$. (IV) *Given two valuations* v_1 *and* v_2 *of* K/k *and an integer* n *such that* $n \not\equiv 0 \pmod{p}$ *in case* $p \neq 0$, *there exists a unique (up to a* K*-isomorphism) tamely ramified cyclic extension* L *of* K *of degree* n *such that* v_1, v_2 *are the only valuations of* K/k *ramified in* L.

Proof. Let $g =$ genus of L/k and $\lambda =$ degree of the difference of L over K. By [Corollary 2, p. 106 of C], $2g = \lambda - 2m + 2$. Since $g \geqq 0$ and $m > 1$ we have $\lambda \geqq 2m - 2 \geqq m > 0$ which proves (I).

Now assume that L/K is tamely ramified, let v be a valuation of K and let $w_1, w_2, \cdots, w_t$ be the valuations of L lying above v; then the contribution $\lambda(v)$ of v to λ is given by $\lambda(v) = \sum_{i=1}^{t} [d(w_i : v) - 1] = m - t \leqq m - 1$. Hence if q valuations of K are ramified in L then $\lambda \leqq q(m-1)$; since $\lambda \geqq 2m - 2 = 2(m-1)$ we must have $q \geqq 2$. Now assume that $q = 2$, let v_1 and v_2 be the valuations of K which are ramified in L, let L^* be a least galois extension of K containing L and let t_1 and t_2 be the number of valuations of L^* lying above v_1 and v_2 respectively, let λ^* be the degree of the different of L^*/K and let $m^* = [L^* : K]$. Then $2m^* - (t^*_1 + t^*_2) = (m^* - t^*_1) + (m^* - t^*_2) = \lambda^* \geqq 2m^* - 2$, hence $t^*_1 = t^*_2 = 1$; therefore the galois group G of L^*/K equals the splitting group S over v_1 of the L^*-extension of v_1. Since v_1 is tamely ramified in L, it follows by Proposition 7 of Section 5 that v_1 is tamely ramified in L^* and hence S is cyclic and $m^* \not\equiv 0 \pmod{p}$. Therefore $L = L^*$. This proves (II) and (III).

A proof of (IV) and a reproof of (II) and (III), all this using only (I), can at once be obtained by the method and results of Section 6.

Remark 5. In the classical case when k is the field of complex numbers, parts (I) and (II) correspond to Proposition T1 and T2 (Section 7), respectively, and parts (III) and (IV) correspond to Proposition T3. II (Section 7).

4. Algebraic fundamental groups and universality. For the sake of definiteness in this section we shall assume that the field of definition of all varieties concerned is a fixed algebraically closed field k of characteristic p.

4.1. *Definitions.* Let F be a *family* of finite groups, given another family F_1 of finite groups we shall regard F and F_1 to be the same families, i.e., $F = F_1$, if f is in F implies there exists f_1 in F_1 isomorphic to f and conversely. Let G be a group (finite or infinite) and let p be a prime number. We make the following definitions:

$(F)^p =$ the family of members of F whose order is prime to p.

$F_s =$ the family of subgroups of members of F.

$F_h =$ the family of homomorphic images of members of F.

$G_h =$ the family of finite homomorphic images of G.

Observe that $F_{shs} = F_{shh} = F_{sh}$ (proof is trivial). Let ϕ be a property of finite groups. F is said to be ϕ if each member of F is ϕ, F is said to be *not* ϕ if at least one member of F is not ϕ, F is said to be *non* ϕ if each member of F is non ϕ. Thus F is abelian means each member of F is abelian, F is not abelian means at least one member of F is nonabelian, and F is nonabelian means each member of F is nonabelian. F is said to be *complete* if F equals the family of *all* finite groups. Observe that many important properties are shared by F, F_s and F_{sh} simultaneously; for instance this is so for the following properties: (1) being abelian, (2) being solvable, (3) being a p-group for a fixed p, (4) being a p-group for various p; i.e., F is abelian if and only if F_s is abelian, if and only if F_{sh} is abelian, and so on. Also note that if $\{F_a\}_{a\in A}$ is a collection of families of finite groups and if the unions are taken over the indexing set A, then $(UF_a)_s = (UF_{as})$, $(UF_{ah}) = (UF_a)_h$ and the same for intersections. For a finite group G we shall denote by $p(G)$ the (normal) subgroup of G generated by all the p-sylow subgroups of G; recall [see A3] that G is called a *quasi* p-group if $G = p(G)$; the family of all quasi p-groups will be denoted by $Q(p)$.

Let V be a normal variety and D a proper subvariety of V. If K^* is a finite algebraic extension of $k(V)$ and V^* is a K^*-normalization of V then the branch locus on V for the transformation between V and V^* will be denoted by $\Delta(V^*/V)$ or by $\Delta(K^*/V)$. Now we define:

(1) $\Omega(V-D) =$ the family of finite algebraic extensions L of $k(V)$ for which $\Delta(L/V) \subset D$.

(2) $\Omega_g(V-D) =$ the family of members L of $\Omega(V-D)$ such that $L/k(V)$ is galois.

(3) $\Omega'_g(V-D) =$ the family of members L of $\Omega_g(V-D)$ such that L/V is tamely ramified.

(4) $\Omega^*_g(V-D)$ = the family of members L of $\Omega_g(V-D)$ such that $[L:k(V)] \not\equiv 0 \pmod p$ in case $p \neq 0$ (and no restriction if $p=0$).

(5) $\pi_A(V-D)$, $\pi'_A(V-D)$, $\pi^*_A(V-D)$
= the family of galois groups of $L/k(V)$ for members L of $\Omega_g(V-D)$, $\Omega'_g(V-D)$, $\Omega^*_g(V-D)$, respectively.

(6) $\pi_B(V-D)$, $\pi'_B(V-D)$, $\pi^*_B(V-D)$
$=[\pi_A(V-D)]_s$, $[\pi'_A(V-D)]_s$, $[\pi^*_A(V-D)]$, respectively.

(7) $\pi_C(V-D)$, $\pi'_C(V-D)$, $\pi^*_C(V-D)$
$=[\pi_B(V-D)]_h$, $[\pi'_B(V-D)]_h$, $[\pi^*_B(V-D)]_h$, respectively.

Now let P be a point on V. Then we define:

(L1) $\Omega(V-D,P)$ = the family of finite algebraic extension L of $k(V)$ for which the components of $\Delta(L/V)$ passing through P are contained in D.

(L2) $\Omega_g(V-D,P)$ = the family of members L of $\Omega(V-D,P)$ such that $L/k(V)$ is galois.

(L3) $\Omega'_g(V-D,P)$ = the family of members L of $\Omega_g(V-D,P)$ such that P is tamely ramified in L.

(L4) $\Omega^*_g(V-D,P)$ = the family of members L of $\Omega_g(V-D,P)$ such that for a point Q corresponding to P on the L-normalization of V we have $d(Q:P) \not\equiv 0 \pmod p$ in case $p \neq 0$ (and no restriction if $p=0$).

(L5) $\pi_A((V-D,P)$, $\pi'_A(V-D,P)$, $\pi^*_A(V-D)$
= the family of splitting groups over $k(V)$ of points corresponding to P on the L-normalization of V for members L of $\Omega_g(V-D,P)$, $\Omega'_g(V-D,P)$, $\Omega^*_g(V-D,P)$, respectively.

(L6) and (L7): Similar to (6) and (7), respectively.

(8) We shall say that $V-D$ is respectively (I) universal, (II) strongly universal, (III) modelwise universal, and (IV) modelwise strongly universal, or, respectively, that (I′) D is a universal branch locus for V,

(II$'$) $\cdots$, (III$'$) $\cdots$, (IV$'$) if, respectively, the following conditions hold: (CI) given a finite algebraic extension K^* of $k(V)$ there exists L in $\Omega(V-D)$ such that L is k-isomorphic to K^*; (CII) given a finite algebraic extension K^*_1 of $k(V)$ and a finite algebraic extension K^*_2 of K^*, there exists L_2 in $\Omega(V-D)$ and L_1 with $K \subset L_1 \subset L_2$ such that there is a k-isomorphism of L_2 onto K^*_2 which maps L_1 onto K^*_1; (CIII) given a finite alegbraic extension K^* of $k(V)$ there exists L in $\Omega(V-D)$ such that the normalizations of V in L and K^* can be mapped onto each other biregularly; (CIV) $\cdots$ such that the normalizations of V in L_2 and K^*_2 can be mapped onto each other by a biregular map which induces a biregular map between the normalizations of V into L_1 and K^*_1. It is clear that (CII) is equivalent to: given a finite sequence of finite algebraic extension $k(V) \subset K^*_1 \subset K^*_2 \subset \cdots \subset K^*_n$, there exist $k(V) \subset L_1 \subset L_2 \subset \cdots \subset L_n$ in $\Omega(V-D)$ and a k-isomorphism of L_n onto K^*_n which maps L_i onto K^*_i for $i=1,2,\cdots,n$; and similarly, for (CIV). Furthermore, D will be said to be a *minimal universal* (respectively strongly universal, modelwise universal, modelwise strongly universal) branch locus for V if D is a universal (respectively s. u., m. u., m. s. u.) branch locus for V and if no proper subvariety of D is such.

Observe that if V is one-dimensional, then things depend only on $k(V)$ and the set of valuations corresponding to the points of D; hence we may replace the models by their function fields.

Having made all these definitions, we now turn to results, conjectures and comments.

4.2. *Fundamental groups.* If k is the field of complex numbers, and if the (corresponding Riemann type) existence theorem for $V-D$ is available, then $(\pi_1(V-D))_h = \pi_A(V-D)$ where π_1 is the topological fundamental group. Although π_1 besides giving $(\pi_1)_h$ also gives the manner in which these groups are intertwined together, nevertheless $(\pi_1)_h$ and hence π_A is a good algebraic approximation to π_1 [of course, eventually one may have to consider the galois group over $k(V)$ of the compositum of all the galois group over $k(V)$ of the compositum of all the members of $\Omega(V-D)$ which one expects to be the Krull-completion of $\pi_1(V-D)$]. For instance, π_1 is free with n generators implies $(\pi_1)_h$ consists of all finite groups with n generators; π_1 is abelian implies $(\pi_1)_h$ is abelian and so on. Since, as has been indicated, important properties are carried simultaneously by π_A, π_B, π_C,

it is quite worthwhile, lacking a knoweldge of π_A itself, to study π_B or π_C. Exactly similar comments are valid for the local situation $V-D,P$.

Concerning ramification theory in the abstract case, we offer the following two general conjectures. For $p\neq 0$ let S_p be a situation either of type $V-D$ or of type $V-D,P$; and let S_0 be the *corresponding situation in characteristic zero* (i.e., in the classical case). Then, roughly speaking:

$$\text{(ramification theory for } S_p) = \text{(ramification theory for } S_0) + Q(P);$$

or better:

$$\text{(ramification theory for } S_p)/Q(P) = \text{(ramification theory for } S_0);$$

and now more precisely:

CONJECTURE 1. *$\pi_A(S_p)$ = the family of all finite groups G such that $p(G)\in Q(p)$ and $G/p(G)\in\pi_A(S_0)^p$.*

CONJECTURE 2 (*Supplement to Conjecture* 1).

$$(\pi_A(S_0))^p = \pi^*{}_A(S_p) \subset \pi'_A(S_p) \subset \pi_A(S_0)$$

and the last inclusion is a near equality.

Conjecture 1 consists of three steps: (1) to algebraize π_1 in the classical case, see Remark 7; (2) to show that *for a situation S_p for which there exist nontrivial coverings, then all members of $Q(P)$ are realizable*; and (3) to do the extension problem for (1) and (2). Let us call step (2), *Conjecture* 1.1; and the much weaker form of 1.1, where we replace $Q(p)$ *by the family of all p-groups*, let it be called *Conjecture* 1.2.

These conjectures on π_A reflect in π_B or π_C in a diluted form. To illustrate the meaning of "corresponding situation" by examples: (1) S_p = line minus n points, S_0 = same; (2) S_p = curve of genus g, S_0 = same; (3) S_p = projective plane minus a curve with ordinary double points and components of orders $n_1, n_2, \cdots, n_t$, S_0 = same; (4) S_p = projective n space minus m hyperplanes in general position, S_0 = same; now some local examples: (5) S_p = (V = projective plane, D = a curve, P = a point at which D has a certain type of singularity), S_0 = ($\cdots$, $\cdots$, $\cdots D$ has the *corresponding* type of singularity). Now for certain situations S_p there may not exist a corresponding S_0; for such S_p the conjectures of course would not apply, for instance in the last example for S_p, P may be a point of D at which there is no Puiseux expansion! For the local theory, a bit of evidence for the conjectures is given in our previous papers [A1] and [A3]; observe that for the local theory, in case of dimension one, $Q(p)$ has

to be replaced by the family of all p-groups [see K]. For the global theory, when V is one-dimensional, the following evidence results from this paper:

Let C be a nonsingular algebraic curve over an algegraically closed ground field k of characteristic p, and let D_n be a set of n (distinct) points of C.

Result 1. In the classical case by Proposition T3, there are only a finite number of (non $k(C)$-isomorphic) members of $\Omega(C-D_n)=\Omega'(C-D_n)$ of a given degree over $k(C)$; by Theorem 5 (Section 6) this is so for any p with $\Omega'(C-D_n)$.

Result 2. (Trivial) $\Omega(C-D_0)$ and $\Omega'(C-D_1)$ are empty (except for C) and $\Omega'(C-D_2)$ consists of all cyclic extensions (of degree prime to p if $p\neq 0$); Proposition 6 and Remark 5 (Section 3).

Now we assume that $C=$ a projective line L (or any rational curve).

Result 3. Let $n\geqq 3$. By Proposition T4 (Section 7) in the classical case $\pi_B(L-D_n)$ is complete. To support the part of Conjecture 2 which says that $\pi'_A(S_p)$ is nearly equal to $\pi_A(S_0)$, we might expect that for arbitrary p not only $\pi_B(L-D_n)$, but even $\pi'_B(L-D_n)$ is complete. *For $p\neq 2$ it follows from Proposition 3 that $\pi'_B(L-D_n)$ is complete, while for $p=2$, Proposition 5 gives the weaker result that $\pi_B(L-D_n)$ is complete* [in fact Proposition 5 yields the stronger conclusion that $\pi_B(L-D_2)$ is complete]. Furthermore by Proposition T3 (Section 7) in the classical case $\pi_A(L-D_n)$ contains all the finite groups generated by two generators and hence in particular for any integer m the symmetric group on m letters: *in the abstract case, we have proved in Proposition 3 that $\pi'_A(L-D_n)$ contains the symmetric group on m letters if $p=0$ and if $p\neq 0$ then provided either $m, m-1\not\equiv 0$* (mod p) *or m is odd and $m, m-2, 2\not\equiv 0$* (mod p).

Result 4. Assume $p\neq 0$. Now Proposition 6 tells us that $\pi_A(L-D_1)\subset Q(p)$ while, in view of Theorem 1, Conjecture 1.1 implies that $\pi_C(L-D_1)=Q(p)\supset$ (family of all simple groups whose orders are divisible by p) $\supset$ the alternating groups on m letters for all $m\geqq p$); this would tend to imply that $\pi_C(L-D_1)$ is complete. Now it does follow from Theorem 2 and Propositions 3 and 5 that *indeed $\pi_C(L-D_1)$ is complete.*

Remark 6. It follows from Result 4 that $\pi_A(L-D_1)$ contains (plenty of them) unsolvable groups, i.e., the affine line $L-D_1$ has unsolvable unramified coverings and hence in particular nonabelian ones. This is

surprising since the affine in line is a commutative group variety. Note that in [L1] Lang had obtained nonabelian coverings only for noncommutative group varieties. It would be interesting to characterize the possible galois groups of unramified coverings of commutative group varieties in general.

Remark 7. The main problem in algebraizing π_1 is to prove Theorem T (Section 7) algebraically, i. e., to prove Theorem T is the abstract case (for any charatceristic) restricting attention to tamely ramified extensions only (in which case we conjecture the theorem to be true). However, even part (III) of Theorem T is false for nontamely ramified extensions, thus: By Remark 6 there exists a galois covering of L with unsolvable galois group G and ramified only in D_1 while the splitting group S of any point above D_1 is solvable [K] and hence S cannot possibly generate G; really! it is unnecessary to be so round-about, for part (III) of Theorem T, if true in general, would imply that if there is only one branch point D_1 on L then D_1 cannot split (by itself); and in Theorem 1 this has been proved false for nontamely ramified extensions. Thus (alas!) for nontamely ramified extensions not only with L with one puncture is nonsimply connected (which has been well known), but the monodromy group is not even generated by the loops around the branch points (Section 7).

4. 3. *Universality.* We may state Theorem 4 as

Result 5. If $p \neq 0$ then for a projective line L over k, any one point of L is a minimal universal as well as minimal strongly universal branch locus for L.

We note that universality is a typical nonzero characteristic concept meaning thereby for characteristic zero one excepts that a universal branch locus could never exist, for instance if L is the projective line over k and D_n a set of n points of L and $p=0$, then (by Theorem 5 of Section 6) the number of non $k(C)$-isomorphic members of $\Omega(L-D_n)$ is countable (i. e., of cardinality less than or equal to that of the set of integers) and *a fortiori* the number of non k-isomorphic members of $\Omega(L-D_n)$ is countable; if now we assume that k is of uncountable cardinality (for instance, $k=$ complex numbers) then there are uncountably many non k-isomorphic extensions of $k(L)$ as follows for instance, since the moduli varieties are positive dimensional varieties over k; hence L has no universal branch locus (this cardinality argument is due to Serre; one should find a proof without the cardinality assumption). However, for a field k of nonzero characteristic, we have

CONJECTURE 3. *Every curve C over k has universal branch loci.*

After proving this conjecture, one should find the comomn properties shared by all the minimal universal branch loci of C; that should yield new (birational) invariants for C. Given a curve over a field of characteristic zero, reducing it modulo various primes would then yield invariants of the original curve for each of these primes. It is clear that if in the definition of universality, we replace overfields by subfields, then there results another concept which we may call *antiuniversality*; it would be interesting to investigate this as well.

5. Least galois extensions. Let K be a one-dimensional algebraic function field over an algebraically closed ground field k of characteristic p. Let L be a finite separable algebraic extension of K and let L^* be a least galois extension of K containing L and let $\Lambda(L/K)$ and $\Lambda(L^*/K)$ denote respectively the differents of L and L^* over K. It is convenient to have a formula expressing $\Lambda(L^*/K)$ in terms of $\Lambda(L/K)$ (it would give the genus of L^* in terms of the genus of K). This can, for instance, be used in studying the following question: What kind of function fields L^* (and what kind of galois groups) can be obtained as the least galois extension of a simple transcendental extension of k containing another simple transcendental extension of k; in other words, given L^*/k under what condition can we find x and t in L^* such that $k(t) \subset k(x)$ and L^* is a least galois extension of $k(t)$ containing $k(x)$? The study of such L^* is facilitated due to the fact that it is gotten by a covering of a line by a line. In this section, we obtain such a formula provided L is tamely ramified over K. Let $v_1, v_2, \cdots, v_t$ be the valuations of K/k which are ramified (tamely) in L; then these are exactly the valuations of K which are ramified in L^* (Proposition 1 of A1). Let $v_{i1}, v_{i2}, \cdots, v_{ia_i}$ be the valuations of L^* lying above v_i and let $w_{i1}, w_{i2}, \cdots, w_{ib_i}$ be the valuations of L^* lying above v_i. Let $d(v_{ij}:v_i) = e_{ij}$ and $d(w_{ij}:v_i) = f_i$ [since L^*/K is galois $d(w_{ij}:v_i)$ does not depend on j]. Then the formula is $f_i = [e_{i1}, e_{i2}, \cdots, e_{ia_i}]$ where the square brackets denote the least common multiple, in other words,

$$\text{if } \Lambda(L/K) = \prod_{i=1}^{t} \prod_{j=1}^{a_i} v_{ij}^{e_{ij}-1}, \text{ then } \Lambda(L^*/K) = \prod_{i=1}^{t} \prod_{j=1}^{b_i} w_{ij}^{[e_{i1}, \cdots, e_{ia_i}]-1}$$

where in each equation the first product sign is taken over all valuations v_i of K/k and the second product sign is taken over all the valuations respectively of L and L^* lying above v_i (for unramified v_i the corresponding exponents of v_{ij} and w_{ij} are zero). This formula is motivated by Proposi-

tion T5 (Section 7) for the classsical case where k is the field of complex numbers and K/k is simple transcendental. Now to the proof. We start with a remark on compositums of fields.

Let K be a field and let $K_1, K_2, \cdots, K_t$ be finite algebraic extensions of K. Recall that an extension K^* of K is called a K-compositum of $K_1, \cdots, K_t$ if K^* contains subfields $K'_1, \cdots, K'_t$ containing K such that K^* is generated over K by $K'_1, \cdots, K'_t$ and K'_i is K-isomorphic to K_i for $i = 1, \cdots, t$. To see that K^* exists it is enough to take an algebraic closure Ω of K, to take for $i = 1, \cdots, t$ subfields K'_i of Ω containing K and K-isomorphic to K_i and to let K^* be the compositum of $K'_1, \cdots, K'_t$ *in* Ω.

Now let $L_1, L_2, \cdots, L_t$ be least normal extension of K containing $K_1, K_2, \cdots, K_t$ respectively. Let L^* be a K-compositum of $L_1, \cdots, L_t$. Then L^*/K is normal (obvious) and is uniquely determined up to isomorphism by the extensions $L_1/K, \cdots, L_t/K$, i.e., if L^{**} is any other K-compositum of $L_1, \cdots, L_t$, then there exists a K-isomorphism τ from L^* onto L^{**} such that if f_i and g_i are the given isomorphisms of L_i onto subfields L'_i and L''_i of L^* and L^{**} respectively, then $f_i\tau = g_i$. For fix a polynomial $A_i(X)$ in $K[X]$ such that L_i is a root field of $A_i(X)$ over K, our assertion then follows from the fact that L'_i is *the* root field of $A_i(X)$ over K *in* L^* [hence $f_i(L_i)$ as a subfield of L^* depends only on L_i and not on f_i] and hence L^* is a root field of $A(X) = A_1(X)A_2(X) \cdots A_t(X)$ over K. The same argument shows that L^* can also be defined as a least normal extension of a K-compositum of $K_1, \cdots, K_t$. We shall call L^* *a least normal K-compositum of* $K_1, \cdots, K_t$.

LEMMA 1. *Let K/k be an r-dimensional algebraic function field, let L be a finite separable algebraic tension of K and let L^* be a least galois extension of K containing L. Let R be the quotient ring of a point on a normal projective model of K/k. Let $S_1, \cdots, S_t$ be the local rings in L lying above R and let S^* be any local ring in L^* lying above R. Let $\bar{R}$ be a completion of R and let $\bar{K}$ be a quotient field of $\bar{R}$ containing K. Let $\bar{S}_i$ be a completion of S_i canonically containing $\bar{R}$ and let $\bar{L}_i$ be a quotient field of $\bar{S}_i$ containing $\bar{K}$ and L. Let $\bar{S}^*$ be a completion of S^* canonically containing $\bar{R}$ and let $\bar{L}^*$ be a quotient field of $\bar{S}^*$ containing $\bar{K}$ and L^*. Then* (I) *$\bar{L}^*$ is a least normal $\bar{K}$-composition of $\bar{L}_1, \bar{L}_2, \cdots, \bar{L}_t$. Let $f(X)$ be the minimal monic polynomial of a primitive element of L/K. Let x be a root of $f(X)$ in L, then* (III) *x as an element of $\bar{L}_i$ is a primitive element of $\bar{L}_i/L$, so that* (IV) *$\bar{L}_i$ is the compositum of L and $\bar{K}$ in $\bar{L}_i$, and if we let $f_i(X)$ be the minimal monic polynomial of x over $\bar{K}$, then* (V)

$f(X)=f_1(X)f_2(X)\cdots f_t(X)$ is the factorization of $f(X)$ into pairwise coprime irreducible factors in $\bar{K}[X]$.

Proof. (III) and (V) are proved in Proposition 1 of [A2] in the case where x is integral over R, however this implies that $\bar{L}_i$ is the compositum of L and $\bar{K}$ *in* $\bar{L}_i$ and hence any primitive element x of L/K is a primitive element of $\bar{L}_i/\bar{K}$ which proves (III) and (IV); again since for a suitable nonzero element c in R, cx is integral over R, Proposition 1 of [A2] gives (V) for cx which in turn implies (V) for x. Now (IV) applied to S^* tells us that $\bar{L}^*$ is the compositum of L^* and $\bar{K}$ in $\bar{L}^*$ and since L^*/L is given by the roots of $f(X)$, we obtain (II). Finally (I) follows from (II) and (V).

LEMMA 2. *Let $E=k((x))$ be the power series field in one variable over an algebraically closed field k of characteristic p and let E^* be a finite algebraic extension of E with $[E^*:E]=n$ such that $n\not\equiv 0 \pmod p$ if $p\neq 0$. Then $E^*=E(x^{1/n})$.*

Proof. This proof is well known.

PROPOSITION 7. *In Lemma 1, assume that k is algebraically closed and $r=1$ and R is tamely ramified in L and let $d(S_i:R)=n_i$. Then $d(S^*:R)=[n_1,n_2,\cdots,n_t]$, (and hence R is tamely ramified in L^*).*

Proof. R is normal, $r=1$ and k is algebraically closed implies that $\bar{K}=k((x))$ where x is a regular parameter in R. By Lemma 2, $\bar{L}_i=\bar{K}(x^{1/n_i})$ and hence by Lemma 1.I, $\bar{L}^*=\bar{K}(x^{1/[n_1,\cdots,n_t]})$ so that $d(S^*:R)=[\bar{L}^*:\bar{K}]$ $[n_1,n_2,\cdots,n_t]$.

Remark 8. Is there a corresponding formula if we omit the assumption of tame ramification?

6. Finiteness of the number of coverings with assigned branch points. In their recent paper, Lang and Serre have proved [Theorem 4 of LS] that if K is a one-dimensional algebraic function field over an algebraically closed ground field k of characteristic p, then for any given integer n the number of non K-isomorphic unramified extensions of K of degree n is finite. Here we extend this result to extensions with assigned branch points (this is done by using a globalized form of a trick which we had used in [A1] for focal purposes), namely

THEOREM 5. *Let V be a given finite set of valuations of K/k and let n be a positive integer. Then the number of non K-isomorphic tamely*

ramified extensions K^* of K of degree n such that $\Delta(K^*/K)$ is contained in V is finite.

We first prove two propositions.

PROPOSITION 8. *Let K^* be a finite separable algebraic extension of a one-dimensional algebraic function field K over an algebraically closed ground field k of characteristic p. For $y \in K$, $y \notin k$, let K^*_1 be a root field of $X^g - y$ over K^* where $g \not\equiv 0 \pmod p$ if $p \neq 0$ and let K_1 be the root field of $X^g - y$ over K in K^*_1. Let v^*_1 be a valuation of K^*_1/k and let v^*, v_1, v be the restrictions of v^*_1 to K^*, K_1, K respectively. Let $h = v(y)$, $n = d(v^*:v)$, $q = (g,h)$, $g_1 = g/q$, $q^* = (g_1, n)$, $N^* = g_1/q^*$ and $N = n/q^*$ [parenthesis denotes the greatest common divisor]. Then (I) $d(v^*_1:v_1) = N$ and $d(v^*_1:v^*) = N^*$. (II) If $h = v(y) = 1$ and $g \equiv 0 \pmod n$ then $N = d(v^*_1:v_1) = 1$. (III) If $d(v^*:v) = 1$ then $d(v^*_1:v_1) = 1$; this remains true if K^*_1 is replaced by any finite separable algebraic extension of K^* and K_1 is replaced by a subfield of K^*_1 containing K such that K^*_1 is the compositum of K_1 and K^*.*

Proof. Fix x in K with $v(x) = 1$. Then $y = x^h\delta$ where $\delta \in K$ with $v(\delta) = 0$. Let z be a root of $X^g - y$ in K^*_1. Let $E = k((x))$ and let E^*_1 be a v^*_1-completion of K^*_1 so that E becomes the corresponding v-completion of K, let E^* and E_1 be the sufields of E^*_1 which are the corresponding completions of K^* and K_1 respectively, then [Proposition 1 of A2] $E^*_1 = E^*(z)$ and $E_1 = E(z)$, also $[E^*_1:E_1] = d(v^*_1:v_1)$, $[E^*_1:E^*] = d(v^*_1:v^*)$ and $[E^*:E] = d(v^*:v) = n$. Since $g \not\equiv 0 \pmod p$ if $p \neq 0$ and δ is a unit in $k[[x]]$, there exists a unit e in $k[[x]]$ such that $e^g = \delta^{-1}$ and we have $(ze)^g = z^g e^g = x^h \delta e^g = x^h$. Hence, by replacing z by ze we may assume that $y = x^h$. Now it follows from Lemma A5 (Section 8) that $[E^*_1:E_1] = N$ and $[E^*_1:E^*] = N^*$ which proves (I), while (II) follows at once from (I). In the present case (III) follows from (I) while in the general case it can be proved directly as follows: Let E^*_1 be a v^*_1-completion of K^*_1 and let E_1, E^*, E be the corresponding completions of K_1, K^*, K respectively. Let z be a primitive element of K^*/K so that z is also a primitive element of K^*_1/K_1 and hence [Proposition 1 of A2] $E^* = E(z)$ and $E^*_1 = E_1(z)$; now $d(v^*:v) = 1$ means $[E^*:E] = 1$, i.e., $z \in E^*$ and hence $z \in E_1$, so that $d(v^*_1:v_1) = [E^*_1:E_1] = 1$.

PROPOSITION 9. *Let K^* be a finite separable algebraic extension of a one-dimensional algebraic function field K over an algebraically closed ground field k of characteristic p. Let L^* be a finite separable algebraic extension*

of K^* and let L be a subfield of L^* containing K such that L^* is the compositum of L and K^*. Let w^* be a valuation of L^*/k and let w, v^*, v be the restrictions of w^* to L, K^*, K respectively. Let $n = d(v^*:v)$. Assume that there exists $z \in L$ and a positive integer g divisible by n with $g \not\equiv 0 \pmod p$ if $p \neq 0$ such that $z^g \in K$ and $v(z^g) = 1$. Then $d(w^*:w) = 1$.

Proof. Let $K_1 = K(z)$, $K^*_1 = K^*(z)$. Apply Proposition 8. II to K^*_1, K_1, K^*, K and then apply Proposition 8. III to L^*, L, K^*_1, K_1.

Proof of Theorem 5. We may restrict our attention to the extensions of K in a fixed algebraic closure Ω of K. It is enough to prove that there exists a finite number of finite separable algebraic extensions $L_1, L_2, \cdots, L_q$ of K such that if K^* is a tamely ramified algebraic extension of K of degree n with $\Delta(K^*/K) \subset V$ then for some L_T the compositum L^*_T of L_T and K^* is unramified over L_T. For then each such K^* will be contained in an unramified extension L^*_T of some L_T with $[L^*_T : L_T] \leqq n$. By the Serre-Lang theorem, the number of these L^*_T is finite for each T and hence the number of fields between L^*_T and K for the various L^*_T for the various L_T $(T = 1, \cdots, q)$ is finite; hence *a fortiori* the number of extensions K^*/K of the said type is also finite.

Proposition 9 gives us various ways of constructing extensions $L_1, \cdots, L_q$ with the required properties. Let $v_1, v_2, \cdots, v_t$ be the valuations in V; fix y_i in K with $v_i(y_i) = 1$. Let $M_T = \{(M_{Ti1}, M_{Ti2}, \cdots, M_{TiT_i})$ $M_{Tij} > 0$, $\not\equiv 0 \pmod p$ if $p \neq 0$; $M_{Ti1} + M_{Ti2} + \cdots + M_{TiT_i} = n$ for $i = 1, 2, \cdots, t\}$ with $T = 1, 2, \cdots, q$ be the various simultaneous (for $i = 1, 2, \cdots, t$; i.e., t at a time) partitions of n into positive integers which are prime to p if $p \neq 0$. For $T = 1, 2, \cdots, q$ let

$$f_T(X) = \prod_{i=1}^{t} \prod_{j=1}^{T_i} (X^{M_{Tij}} - y_i),$$

and let L_T be the root field of $f_T(X)$ over K. Then given K^* (of the said type) there is a (unique) T such that for $i = 1, 2, \cdots, t$ the degrees over v_i of the various extensions of v_i to K^* are $M_{Ti1}, M_{Ti2}, \cdots, M_{TiT_i}$; and hence by Proposition 9, the compositum of L_T and K^* is unramified over L_T.

Also we can, in various ways, manage that it will be enough to take one single L. Firstly, we can take for L the root field over K of $f_1(X) f_2(X) \cdots f_q(X)$. Secondly, letting N to be the product of all positive integers which are less than or equal to n and which are prime to p if $p \neq 0$, we can take for L the root field over K of $(X^N - y_1)(X^N - y_2) \cdots (X^N - y_t)$. Thirdly, by the theorem of independence of valuations there exists $y \in K$

such that $v_i(y)=1$ for $i=1,2,\cdots,t$; and we may take for L the root field of X^N-y over K.

That the condition of tame ramification is essential is well known. For instance, let $K=k(x)$ be simple transcendental with k algebraically closed of characteristic $p\neq 0$ and let K^*_m be a root field over K of $f_m(X)=X^p-X-x^m$ where m is any positive integer prime to p. Then K^*_m/K is cyclic of degree p. Since $f'_m(X)=-1$, $v: x=\infty$ is the only valuation of K/k which is possibly ramified in K^*_m. Let z be a root of $f_m(X)$. Then $K^*_m=k(z)(x)$ and $g_m(X)=X^m+z-z^p$ is the minimal monic polynomial of x over $k(z)$. Let w_i be the valuation of $k(z)/k$ given by $z=i$ for $i=1,2,\cdots,p$ and let w_∞ be the valuation of $k(z)/k$ given by $z=\infty$. Then $Dg_m(X)=(z-z^p)^{m-1}$ so that $w_1,\cdots,w_p,w_\infty$ are the only valuations of $k(z)/k$ which are possibly ramified in K^*_m. Also $w_i(x^m)=1$ for $i=1,\cdots,p$ and $w_\infty(x^m)=-1$ imply that there are unique valuations $w^*_1,\cdots,w^*_p,w^*_\infty$ of K^*_m lying above $w_1,\cdots,w_p,w_\infty$ respectively and $d(w^*_i:w_i)=m\not\equiv 0 \pmod p$ for $i=1,2,\cdots,p,\infty$. Therefore the genus g_m of K^*_m/k is given by: $g_m=(\frac{1}{2})(p+1)(m-1)-m+1=(\frac{1}{2})(p-1)(m-1)$. Hence for the various values of m the extensions K^*_m are of distinct genera so that they are non k-isomorphic and hence *a fortiori* non K-isomorphic.

Remark 9. Presumably one can at once generalize Theorem 5 to higher dimensional varieties by taking a generic plane section and applying Theorem 5.

7. Some topological considerations in the classical case. In this section, we shall not try to be completely precise since logically the contents of this section do not belong in this paper and are used only for descriptive, motivating, and comparative purposes. For well-known properties of topological coverings to be used, we refer for instance to Part I of [S2].

Let K be a pure transcendental extension of the field k of complex numbers, and let L be a finite algebraic extension of K with $[L:K]=n>1$. Let T be the Riemann surface of L/k, i.e., the set of all valuations of L/k topologized in the classical fashion and let S be the Riemann surface of K/k; then S is the Riemann sphere and T is a ramified covering of S, let f be the projection of T onto S, let D be the set of points of S which are ramified in L and let E be the set of points of T lying above the points of D, then $T-E$ is an unramified covering of $S-D$; we may think of S as the euclidean plane R together with a point P_∞ at infinity. Since S as well as R are simply connected, D must contain more than one point and we may state

PROPOSITION T1. *There are no unramified proper extensions of K/k.*

PROPOSITION T2. *There are no proper extensions of K/k which are ramified only at one valuation of K/k.*

Let γ be an arc in $S-D$ from a point X_0 to a point X_1, let Y_0 be any point in $f^{-1}(X_0)$, then there exits a unique arc δ in $T-E$ starting at Y_0 and lying over γ, let Y_1 be the point of δ lying avove X_1; thus γ gives rise to a mapping of $f^{-1}(X_0)$ into $f^{-1}(X_1)$ which we shall denote by $h(\gamma)$; observe that h is multiplicative; now $h(\gamma)$ does not change if we vary γ by a homotopy (stationary at X_0 and X_1) and hence we obtain a mapping from the homotopy classes of arcs in $S-D$ into the class of mappings of the fibres of their starting points into the fibres of their end points; this mapping we shall also denote by h; the restriction of h to the loops at a point X_0 then gives the homomorphism of $\pi_1(S-D, X_0)$ into the group of permutations of $f^{-1}(X_0)$ and this will again be denoted by h; which particular meaning of h is to be taken will always be obvious from the context. For a point X_0 in $S-D$ we shall denote $h(\pi_1(S-D, X_0)$ by $H(X_0)$. Let P be a given point in D, we may assume that P_∞ is any point of D other than P; let $Q_1, Q_2, \cdots, Q_t$ be the points in $f^{-1}(P)$ and let $d(Q_i:P)=r_i$. Let A be a small closed circular neighborhood with center P (not containing any other points of D); then the use of uniformizing parameters at once shows that the connected components of $f^{-1}(A)$ are neighborhoods $B_1, B_2, \cdots, B_t$ of $Q_1, Q_2, \cdots, Q_t$ respectively and B_i-Q_i is an r_i-fold cyclic covering of $A-P$. Let a be the positively oriented (with respect to a fixed orientation of S) boundary of A. Let M be a point on a and let $N_{i1}, N_{i2}, \cdots, N_{ir_i}$ be the points in B_i lying above M. Now a is a deformation retract of $A-P$ stationary at M and hence a generates $\pi_1(A-P, M)$. Therefore the action of a on $N_{i1}, N_{i2}, \cdots, N_{ir_i}$ is to permute them cyclically, i.e., if for each fixed i we arrange the N_{ij} suitably, then the action of a is given by the r_i-cycle $(N_{i1}, N_{i2}, \cdots, N_{ir_i})$. Hence the action of a on $f^{-1}(M)$, i.e., $h(a)$, is the permutation on the $r_1+r_2+\cdots+r_t=n$ points N_{ij} which is the product of the t disjoint cycles $(N_{i1}, N_{i2}, \cdots, N_{ir_i})$, $i=1,2,\cdots,t$. Now let M_0 be any point of $S-D$, let u be any arc from M_0 to M in $S-D$, and let $\alpha=uau^{-1}$. Then $h(\alpha)$ is gotten from $h(a)$ by a one-to-one mapping from $f^{-1}(M)$ onto $f^{-1}(M_0)$. Hence we have

LEMMA T1. *The canonical decomposition of $h(\alpha)$ into disjoint cycles consists of cycles of orders $r_1, r_2, \cdots, r_t$.*

Now let $P=P_1, P_2, \cdots, P_q, P_\infty$ be a labelling of the points of D.

Let a_i be the positively oriented boundary of a small circle A_i around P_i $(i=1,2,\cdots,q)$, let M_0 be a point in $S-D$ not on any line passing through any two of the points $P_1,P_2,\cdots,P_q$; let M_i be the points of intersection of M_0P_i with a_i, let u_i be the straight line from M_0 to M_i, and let $\alpha_i=u_ia_iu_i^{-1}$; let a_∞ be the positively oriented circumference of a large circle A_∞ containing $\alpha_1,\alpha_2,\cdots,\alpha_q$ (which is thus a *small* circle around P_∞), let u_∞ be a straight line from M_0 to a point M_∞ on a_∞ such that u_∞ such that u_∞ does not meet any of the α_i and let $\alpha_\infty=u_\infty a_\infty u_\infty^{-1}$. Arrange the labelling of the P_i so that $u_1,u_2,\cdots,u_q,u_\infty$ are consecutive lines through M_0. (The reader may draw a diagram.) Then it can easily be seen that

LEMMA T2. *α_∞ is homotopic to $\alpha_1\alpha_2\cdots\alpha_q$ (with M_0 fixed).*

Also the one-dimensional (cell) complex $J=\alpha_1\cup\alpha_2\cup\cdots\cup\alpha_q$ is a deformation retract of $R-D=S-D$ and $\pi_1(J,M_0)$ is the free group generated by $\alpha_1,\alpha_2,\cdots,\alpha_q$ (or loosely speaking: by $a_1,a_2,\cdots,a_q$) and hence we have

LEMMA T3. *$\pi_1(S-D,M_0)$ is the free group generated by $\alpha_1,\alpha_2,\cdots,\alpha_q$.*

Hence we have

PROPOSITION T3. (I) *$\pi_1(S-(q+1)$ points) is the free group F_q on q generators. In particular* (II) *$\pi_1(S-2$ points) is infinite cyclic and* (III) *$\pi_1(S-3$ points) is the free group F_2 on two generators.*

Corollary. A proof of Schreier's theorem. By Proposition 4, $S-3$ points can be covered by $S-(q+1)$ points for (arbitrarily) large q, hence $F_q=\pi_1(S-(q+1)$ points$)\subset\pi_1(S-3$ points$)=F_2$ for (arbitrarily) large q and hence $F_q\subset F_2$ for *all* q.

Moreover, by Proposition 4, for large q, $S_{q+1}=S-(q+1)$ points in a *finite* unramified covering of $S_3=S-3$ points; given a finite unramified regular covering Γ of S_{q+1} we may pass to the least regular unramified covering Γ^* of S_3 *dominating* Γ, then Γ^* is a finite covering of S_3 and the deck group of Γ over S_{q+1} is the homomorphic image of a subgroup of the deck group of Γ^* over S_3; since in Proposition 4 we could replace S_3 by S_n for any $n\geqq 3$, then denoting the free group on n generators by F_n, we have that $(F_{n-1})_{hsh}=(\pi_1(S_n))_{hsh}$ is complete. However if we observe that any finite group is isomorphic to a permutation group and that the symmetric group on any number of letters can be generated by two generators and that $(\pi_1(S_n))_{hs}\supset(\alpha_1(S_3))_{hs}$ there results a stronger assertion, namely

PROPOSITION T4. *For $n \geqq 3$, $(\pi_1(S - n \text{ points}))_{hs}$ is complete.*

Now let L^* be a least normal extension of K containing L, let G be the galois group of L^*/K, let $[L^*:K] = n^*$. Let $T^*, f^*, E^*, h^*, H^*(X_0)$, $Q^*_1, Q^*_2, \cdots, Q^*_{t^*}$, $r^*_1, r^*_2, \cdots, r^*_{t^*}$ be the entities gotten from T, F, E, h, $H(X_0)$, $Q_1, Q_2, \cdots, Q_t$, $r_1, r_2, \cdots, r_t$ respectively by replacing L by L^*. Since L^*/K is normal, $r^*_1 = r^*_2 = \cdots = r^*_{t^*}$, let r^* be this common value. Let B^*_i be the connected component of $f^{*-1}(A_1)$ containing Q^*_i.

Let X_0 be any point of $S - D$. Recall that $H(X_0)$ is a permutation group of $f^{-1}(X_0)$; it is called the monodromy group of T over S. It is well-known that $H(X_0)$ is isomorphic to G; a classical proof can be found in any older treatise, secondly a modernistic proof in terms of associated principal bundles [S2] can be easily reconstructed, and thirdly the required isomorphism x of G onto $H(X_0)$ may be obtained thus: by the approximation theorem for valuations, we can find ξ in L whose values at the various points of $f^{-1}(X_0)$ are distinct, then for e in $H(X_0)$ define $x^{-1}(e)$ by setting $Y[x^{-1}(e)\xi] = e(Y)[\xi]$ for all Y in $f^{-1}(X_0)$ (if we replace the points of $f^{-1}(X_0)$ by their associated places, instead of the approximation theorem of valuations it would be enough to use the independence of places), observe that then for any $\eta \in L$, $g \in G$ and $Y \in f^{-1}(X_0)$ we have $Y[g(\eta)] = (x(g)Y)[\eta]$.

Replacing L by L^* and X_0 by M_0, we obtain an onto isomorphism $x^*: G \to H^*(M_0)$. Let $\bar{V}$ and V be the groups of fibre preserving (over S) auto-homeomorphisms respectively of $T^* - E^*$ and T^*; by continuity, extension and restriction give an isomorphism between $\bar{V}$ and V. Since $T^* - E^*$ is a regular covering of $S - D$, if we fix a point N^*_0 in $f^{*-1}(M_0)$ we obtain a unique onto isomorphism $y^*: H^*(M_0) \to \bar{V}$ as follows: let $e \in H^*(M_0)$ and $Y^* \in T^* - E^*$ be given; let $X = f^*(Y^*)$, fix a loop β in $S - D$ at M_0 with $h^*(\beta) = e$ and fix an arbitrary arc δ^* in $T^* - E^*$ from Y^* to N^*_0 and let $\gamma = f^*(\delta)$, then $[y^*(e)][Y^*] = [h^*(\gamma\beta\gamma^{-1})](Y^*)$. Now y^* gives an onto isomorphism: $H^*(M_0) \to V$ which we again denote by y^*. Thus we have an onto isomorphism $y^*x^*: G \xrightarrow{x^*} H(M_0) \xrightarrow{y^*} V$; observe that for $g \in G$ and $Y^* \in T^*$ we simply have $[y^*x^*(g)](Y^*) = g(Y^*)$, ($Y^*$ is a valuation of L^*).

Let v_1 be the unique arc in $T^* - E^*$ starting from N^*_0 lying above u_1 and let N^*_1 be the point of v_1 lying above M_1, then $N^*_1 = [h^*(u_1)](N^*_0)$. Let B^*_i be the connected component of $f^{*-1}(A_1)$ containing N^*_1. Let $\mu = u_1^{-1}\alpha_1 u_1$, then $y^*(h^*(\alpha_1))(N^*_1) = h^*(\mu)(N^*)$. Now $\mu = u_1^{-1}\alpha_1 u_1$ $= u_1^{-1}u_1 a_1 u_1^{-1} u_1 = a_1$ and hence $y^*(h^*(\alpha_1))(N^*_1) = h^*(a_1)(N^*_1) \in B^*_i$. Therefore $y^*(h^*(\alpha_1))(Q^*_i) = Q^*_i$. By Lemma T1 the canonical decom-

position of $h^*(\alpha_1)$ consists of r^*-cycles and hence the order of $h^*(\alpha_1)$, i.e., the order of $y^*(h^*(\alpha_1))$ is r^*. Let g_1 be the element of G which goes into $y^*(h^*(\alpha_1))$ under the isomorphism y^*x^*, then $g_1 = x^{*-1}y^{*-1}y^*h^*(\alpha_1) = x^{*-1}(\alpha_1)$, g_1 is of order r^* and g_1 maps the valuation Q^*_i of L^* onto itself, since the splitting group of Q^*_i over P_1 is of order r^*, g_1 must generate this group.

Similarly for $i = 1, 2, \cdots, q, \infty$ if we let $g_i = x^{*-1}(\alpha_i)$, there exists a valuation $\bar{Q}^*_i$ of L^* are lying above P_i such that g_i generates the splitting group of $\bar{Q}^*_i$ over P_i. Now suppressing the bar over $\bar{Q}^*_i$ and observing that the splitting groups of all the points of T^* lying above a given point of S form a complete conjugate set of subgroups of G, we conclude by Lemmas T2 and T3 the following

THEOREM T. *Let k be an algebraically closed field of characteristic zero having the cardinality of the continuum, let K be a simple transcendental extension of k, let L^* be a finite normal extension of K and let G be the galois group of L^*/K. Let $P_1, P_2, \cdots, P_{q+1}$ be the valuation of L^* lying above P_1. Then there exist valuations $Q^*_2, Q^*_3, \cdots, Q^*_{q+1}$ of L^* lying above $P_2, P_3, \cdots, P_{q+1}$ respectively and a generator g_i of the splitting group of Q^*_i over P_i for $i = 1, 2, \cdots, q+1$ such that* (I) $g_1 g_2 \cdots g_{q+1} = 1$ *and any q of the g_i generate G. In particular* (II) *the splitting groups of any q of the $q+1$ points Q^*_i (over the corresponding points P_i) generate G and hence a fortiori* (III) *the splitting groups of all the $q+1$ points Q^*_i generate G.*

Now observe that the order of $H(M_0) =$ order of $G = [L^*:K] = n^*$ ond fixe loops $\gamma_1, \gamma_2, \cdots, \gamma_{n^*}$ in $S - D$ at M_0 such that the elements $e_1 = h(\gamma_1), e_2 = h(\gamma_2), \cdots, e_{n^*} = h(\gamma_{n^*})$ are all distinct and hence these are all the elements of $H(M_0)$. Since $T^* - E^*$ is an unramified covering of $T - E$ it follows that $h^*(\gamma_1), h^*(\gamma_2), \cdots, h^*(\gamma_{n^*})$ are all distinct and hence these are all the elements of $H^*(M_0)$. Recall that N^*_0 is a fixed point in $f^{*-1}(M_0)$. Let $N^*_i = h^*(\gamma_i)N^*_0$. Then $N^*_1, N^*_2, \cdots, N^*_{n^*}$ are all distinct and these are all the points of $f^{*-1}(M_0)$. Now

$$h^*(\gamma_i\gamma_j)N^*_0 = h^*(\gamma_j)[h^*(\gamma_i)N^*_0] = h^*(\gamma_j)N^*_i$$

and hence if we identify $\gamma_1, \gamma_2, \cdots, \gamma_{n^*}$ respectively with $e_1, e_2, \cdots, e_{n^*}$ and $N^*_1, N^*_2, \cdots, N^*_{n^*}$ respectively with $h^*(\gamma_1), h^*(\gamma_2), \cdots, h^*(\gamma_{n^*})$, there results the following: $H^*(M_0)$ is the right regular representation of $H(M_0)$. Hence by Lemma T1: [least comon multiple of $r_1, r_2, \cdots, r_t$] = [order of $h((_1)]$ = [the order of a cycle in the canonical decomposition of $h^*(\gamma_1)$] $= r^*$. Hence we may state

PROPOSITION T5. *Let K/k and L^* be as in Theorem* T *and let L be a field between K and L^* such that L^* is a least normal extension of K containing L. Let P be a valuation of K/k, let $Q_1, Q_2, \cdots, Q_t$ be all the valuations of L lying above P and let Q^* be any valuation of L^* lying above P. Then $d(Q^*:P)=$ the least common multiple of $d(Q_1:P), d(Q_2:P), \cdots, d(Q_t:P)$.*

8. Appendix. We put together here the proofs of some of the lemmas we have used.

LEMMA A1. *Let $G(Z)=Z^g+G_1(X)Z^{g-1}+G_2(X)Z^{g-2}+\cdots+G_g(X)$ with $G_i(X)\in k[[X]]=k[[X_1,X_2,\cdots,X_t]]$ where k is an arbitrary field. Assume that $|G_i(X)|_X\geqq i$ for $i=1,2,\cdots,g-1$ and $|G_g(X)|_X=g-1$. Then $G(Z)$ is irreducible in $k[[X]][Z]$.*

Proof. Suppose if possible that $G(Z)=H(Z)K(Z)$ with

$$H(Z)=Z^h+H_1(X)Z^{h-1}+H_2(X)Z^{h-2}+\cdots+H_h(X), H_i(X)\in k[[X]];$$

$$K(Z)=Z^k+K_1(X)Z^{k-1}+K_2(X)Z^{k-2}+\cdots+K_k(X), K_i(X)\in k[[X]].$$

Let $H^*(Z,X)$ and $K^*(Z,X)$ be the leading forms respectively of $H(Z)$ and $K(Z)$ considered as elements of $k[[X,Z]]$. Then $H^*(Z,X)$ and $K^*(Z,X)$ are in $k[[X]][Z]$. Let $G^*(X)$ be the leading form of $G_g(X)$. Since

$$|G_g(X)|_{X,Z}=g-1<g=\min[|Z^g|_{X,Z}, |G_1(X)Z^{g-1}|_{X,Z},\cdots,|G_g(X)|_{X,Z}],$$

$G^*(X)$ is also the leading form of $G(Z)$ as an element of $k[[X,Z]]$. Hence $H^*(Z,X)K^*(Z,X)$ are in $[[X]]$. Hence $H^*(Z,X)=$ leading form of $H_h(X)$, and $K^*(Z,X)=$ leading form of $K_k(X)$. Hence $h=|Z^h|_{X,Z}>|H_h(X)|_{X,Z}=|H_h(X)|_X$ so that $h-1\geqq|H_h(X)|_X$. Similarly $k-1\geqq|K_k(X)|_X$. Therefore

$$g-2=h+k-2=|H_h(X)|_X+|K_k(X)|_X=|H_h(X)K_k(X)|_X$$
$$=|G_g(X)|_X=g-1.$$

This is a contradiction and the lemma is established.

LEMMA A2. *Let $F(Z)=Z^{p+1}+x^{p-1}Z+x^{p+1}\in k[[x]][Z]$ and let $H(Z)=Z^p+x^2Z^{p-1}+x^{p-1}$ where k is an algebraically closed field of characteristic $p\neq 0$. The galois groups of $F(Z)$ and $H(Z)$ over $k((x))$ are isomorphic as permutation groups.*

Proof. By equation (7) of Section 2, $F(Z) = G(Z)(Z + ux^2)$, where $u \in k[[x]]$ and $G(Z)$ is an irreducible monic polynomial in $k[[x]][Z]$; the isomorphism in the statement of the lemma is to be interpreted as an isomorphism between the galois groups of $G(Z)$ and $H(Z)$ over $k((x))$ as premutation groups.

Let $Z_1 = Z + ux^2$, $F_1(Z_1) = F(Z)$, $H_1(Z_1) = G(Z)$. Then

$$\begin{aligned} F_1(Z_1) = F(Z) = F(Z_1 - ux^2) &= (Z_1 - ux^2)[(Z_1 - ux^2)^p + x^{p-1}] + x^{p+1} \\ &= (Z_1 - ux^2)[Z_1^p - u^p x^{2p} + x^{p-1}] + x^{p+1} \\ &= Z_1^{p+1} - ux^2 Z_1^p + x^{p-1}(1 - u^p x^{p+1}) Z_1 + F_1(0) \end{aligned}$$

$$= Z_1[Z_1^p - ux^2 Z_1^{p-1} + x^{p-1}(1 - u^p x^{p+1})], \text{ since } F_1(0) = F(-ux^2) = 0.$$

Therefore

$$H_1(Z_1) = Z_1^p + dx^2 Z_1^{p-1} + ex^{p-1},$$

where d and e are units in $k[[x]]$. Let $Z_1 = Z^*\delta_1$ and $x = x^*\delta_2$ where δ_1 and δ_2 are units in $k[[x]]$ to be chosen. Now

$$\begin{aligned} H_1(Z_1) &= \delta_1^p Z^{*p} + d\delta_1^{p-1}\delta_2^2 x^{*2} Z^{*p-1} + e\delta_2^{p-1} x^{*p-1} \\ &= \delta_1^p (Z^{*p} + d\delta_1^{-1}\delta_2^{-2} Z^{*p-1} + e\delta_1^{-p}\delta_2^{p-1} x^{*p-1}). \end{aligned}$$

We want

(1) $$d\delta_1^{-1}\delta_2^2 = 1 \text{ and } e\delta_1^{-p}\delta_2^{p-1} = 1$$

i. e.,

(2) $$\delta_1 = d\delta_2^2 \text{ and } \delta_2^{p-1} = e^{-1}\delta_1^p.$$

Equations (2) imply: $\delta_2^{p-1} = e^{-1}d^p\delta_2^{2p}$ which in turn implies $\delta_2^{p+1} = ed^{-p}$. Now $(ed^{-p})(0) = e(0)d(0)^{-p} = e(0)u(0)^{-p} = 1$. Sincs $p + 1 \not\equiv 0 \pmod p$, by Hensel's Lemma, we can find a unit δ_2 in $k[[x]]$ with $\delta_2(0) = 1$ and $\delta_2^{p+1} = ed^{-p}$. Substituting in the first equation of (2), we let $\delta_1 = d\delta_2^2$. Then the required equations (1) are satisfied and we have

$$\delta_1^{-p} G(Z) = \delta_1^{-p} H_1(Z_1) = Z^{*p} + x^{*2} Z^{*p-1} + x^{*p-1}.$$

LEMMA A3. *Let k be an arbitrary field, let y be a transcendental over k and let u_1, u_2, u_3 be any three distinct valuations of $k(y)/k$ rational over k. Then there exists a generator z of $k(y)/k$ such that u_1: $z = 0$, u_2: $z = 1$ and u_3: $z = \infty$. Hence if v_1, v_2, v_3 are any three distinct rational valuations of $k(y)/k$, then there exists a k-automorphism of $k(y)$ which maps u_i onto v_i for $i = 1, 2, 3$.*

Proof. If u_3 is not $y = \infty$ then there exists unique c in k such that

$u_3(y-c)=1$, let $y'=1/(y-c)$; then $k(y')=k(y)$ and u_3 is $y'=\infty$; hence to begin with, we may assume that u_3 is $y=\infty$. Then there exists a unique d in k with $u_1(y-d)=1$; replacing y by $y-d$ we may assume that u_1 is $y=0$. Then there exists a unique e in k with $e\neq 0$ and $u_2(y-e)=1$. It is enough to take $z=(1/e)y$.

LEMMA A4. *Let G be a finite group and p a prime number. Assume that G has only one p-sylow subgroup S (which is therefore a normal subgroup of G). Let H be a given subgroup of G and let $[G:H]=n=mp^a$ with $m\not\equiv 0(p)$.*[2] *Then $[G:HS]=m$, i.e., $[HS:H]=p^a$, and HS is the only such subgroup of G containing H. If G/S is abelian, then HS is a normal subgroup of G.*

Proof. Let $[H:1]=n'=m'p^{a'}$ with $m'\not\equiv 0(p)$. Then $[G:1]=nn'=mm'p^{a+a'}$ and $mm'\not\equiv 0(p)$ so that $[S:1]=p^{a+a'}$. Let S^* be a p-sylow subgroup of H; then the order of S^* is $p^{a'}$. Since S is the only p-sylow subgroup of G, $S^*\subset S$ (Theorem 4, p. 107 of [Z]) and hence $S^*=S\cap H$. Therefore HS/S is isomorphic to H/S^* and hence $[HS:S]=[H:S^*]=m'$ so that $[G:HS]=[G:S]/[HS:S]=(mm')/m'=m$. If G^* is a subgroup of G containing H such that $[G:G^*]=m$, then $[G^*:1]=m'p^{a+a'}$ and hence the unique p-sylow subgroup S of G must be contained in G^* and hence $G^*\supset HS$; since $[G:G^*]=m=[G:HS]$ we must have $G^*=HS$. If G/S is abelian, HS/S is a normal subgroup of G/S and hence HS is a normal subgroup of G.

LEMMA A5. *Let $E=k((x))$ where k is algebraically closed of characteristic p. Let E^* be a finite separable algebraic extension of E, let $[E^*:E]=n$ and $n=mp^a$ with $m\not\equiv 0(p)$ if $p\neq 0$ and $n=m$ if $p=0$. Then $x^{1/m}\in E^*$ so that $[E^*:F]=p^a$ and $[F:E]=m$ where $F=k((x^{1/m}))=E(x^{1/m})$. Let E^*_1 be a root field of X^g-x^h over E^* where g and h are integers, g is positive and $g\not\equiv 0(p)$ if $p\neq 0$; let E_1 be the root field of X^g-x^h over E in E^*_1; let $q=(g,h)$, $g_1=g/q$, $q^*=(g_1,n)$, $N^*=g_1/q^*$ and $N=n/q^*$. Then $[E^*_1:E_1]=N$ and $[E^*_1:E^*]=N^*$.*

Proof. For $p=0$, everything follows from well-known theorems, so assume $p\neq 0$. Let E' be a galois extension of E^* containing E, let G be the galois group of E' over E and let H be the galois group of E' over E^*. Then G contains a unique p-sylow subgroup S and G/S is cyclic (see [K]). Let F be the fixed field of HS. Then by Lemma A4, $[F:E]=m\not\equiv 0(p)$

[2] For a subgroup H of a finite group G we shall denote the index of H in G by $[G:H]$.

and hence $F = E(x^{1/m})$. To prove the second part, let z be a root of $X^g - x^h$. Then $E^*_1 = E^*(z)$ and multiplying z by a root of unity, we may assume that $z^{g_1} = x^{h_1}$ where $h_1 = h/q$. Then $(g_1, h_1) = 1$ and hence (as in Section 5 of [A2]) we may arrange matters so that $h_1 = 1$. Since by the first part we know that $x^{1/m}$ is the lowest positive power of x in E^* and since $q^* = (g_1, n) = (g_1, m)$, we conclude that $X^{N^*} - x^{1/q}$ is the minimal polynomial of z over E^*. Therefore $[E^*_1 : E^*] = N^*$. Hence $[E^*_1 : E_1] = [E^*_1 : E][E_1 : E]^{-1} = [E^*_1 : E^*][E^* : E][E_1 : E]^{-1} = N^* n g_1^{-1} = g_1 q^{*-1} n g_1^{-1} = N$.

COLUMBIA UNIVERSITY.

REFERENCES.

[A1] S. Abhyankar, "On the ramification of algebraic functions," *American Journal of Mathematics*, vol. 77 (1955), pp. 575-592.

[A2] ———, "Local uniformization on algebraic surfaces over ground fields of characteristic $p \neq 0$," *Annals of Mathematics*, vol. 63 (1956), pp. 491-526.

[A3] ———, "On the ramification of algebraic functions, Part II: Unaffected equations for characteristic two," forthcoming in the Transactions of the American Mathematical Society.

[C] C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, New York, 1951.

[D] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper," *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, vol. 14 (1941), pp. 197-272.

[H] H. Hasse, "Existenz separabler zyklischer unverzweigter Erweitungskörper vom Primzahlgrade p über elliptnschen Funktionenkörpern der Charakteristic p," *Crelle Journal*, vol. 172 (1934), pp. 77-85.

[K] W. Krull, "Galoissche Theorie bewerteter Körper," *Sitzungsberichte der Bayerschen Akademie des Wissenschaften*, 1930, pp. 225-238.

[L1] S. Lang, "Algebrais groups over finite fields," *American Journal of Mathematics*, vol. 78 (1956), pp. 555-563.

[L2] ———, "Sur le séries L d'une variété algébrique," *Bulletin de la Société Mathematique de France*, vol. 84 (1956), pp. 385-407.

[LS] ———, and J.-P. Serre, "Sur les revêtments non ramifiés des variétés algébriques." *American Journal of Mathematics*, vol. 79 (1957), pp. 319-330.

[O] A. Ostrowski, "Untersuchungen zur arithmetischen Theorie der Körper," *Mathematische Zeitschrift*, vol. 39 (1934), pp. 269-404.

[S1] J.-P. Serre, "Sur la topologie des variétés algébrique en characteristic p," Symposium of algebraic topology, Mexico (1956).

[S2] N. Steenrod, *The topology of fibre bundles*, Princeton, 1951.

[V] B. L. van der Waerden, *Modern Algebra*, vol. I, New York, 1949.

[Z] H. Zassenhaus, *The theory of groups*, New York, 1949.

VARIATIONAL METHODS IN ENTIRE FUNCTIONS.*

By R. P. Boas, Jr. and A. C. Schaeffer.[1]

1. Introduction. Consider the class of entire functions $f(z)$ of exponential type τ, such that $|f(x)| \leqq M$ for all real x. We ask for the smallest $A_n(\tau)$ such that

$$(1.1) \qquad |\sum_{k=0}^{n} f'(k+x)| \leqq A_n(\tau) M$$

for all f in the class. By S. Bernstein's famous theorem (see, e.g., [2], p. 206), $A_n(\tau)$ does not exceed $(n+1)\tau$. In another paper [3] we have shown that $A_n(\tau) \leqq \pi$ when $\tau \leqq \pi$; the example $f(z) = \sin \pi z$ shows that this estimate is sharp when n is even, but we have shown that it is not sharp when n is odd; in particular, $A_1(\pi) < 8/\pi < \pi$. In the present paper we attack the problem of finding the best possible $A_n(\tau)$. It is not difficult to show that, for a given x_0, there is a function $f_0(z)$ for which (1.1) becomes an equality. We shall show by variational methods that $f_0(z)$ satisfies a differential equation which is generally hyperelliptic; the determination of $A_n(\tau)$ is then reduced to the investigation of solutions of this differential equation. We shall develop the variational methods for a more general case, since they can be used for other questions in the theory of entire functions. There are analogous questions for polynomials, which have been investigated by Chebyshev [4] and Zolotarev [6].

For $n=1$ (that is, for $|f'(x) + f'(x+1)|$) we can give the extremal function fairly explicitly for every τ, although for some values of τ it is expressed in terms of elliptic integrals and we do not obtain an explicit formula for $A_n(\tau)$. A detailed statement is given in Section 10. As simpler applications of the variational method we determine the maximum of $|\lambda f(x) + f''(x)|$ (§ 8) and of $|f'(x) - f'(x+1)|$ (§ 9).

---

* Received February 18, 1957.

[1] This represents work done by Boas with partial support of the National Science Foundation and by Schaeffer under Contract N7 onr-28507 with the Office of Naval Research.

2. The variational problem. Let $\mathcal{L}$ be the linear functional defined by

$$\mathcal{L}(f) = \sum_{\nu=1}^{m} \sum_{j=0}^{n_\nu} \alpha_\nu^{(j)} f^{(j)}(x_\nu), \tag{2.1}$$

where $x_1, \cdots, x_m, \alpha_\nu^{(j)}$ are given real numbers, with the x_ν all different. We suppose that $\alpha_\nu^{(n_\nu)} \neq 0$, and that $n_\nu > 0$ for at least one ν. We call

$$l = n_1 + n_2 + \cdots + n_m + m$$

the order of the functional $\mathcal{L}$. Thus $f'(\frac{1}{2}) + f'(-\frac{1}{2})$ is a functional of order 4.

We wish to investigate the existence and properties of the entire function $f(z)$, of exponential type τ, bounded by 1 on the real axis, for which $|\mathcal{L}(f)|$ is largest. We may, without loss of generality, restrict our attention to functions which are real for real z. For, if θ is real, we have $e^{i\theta}f(z) = f_1(z) + if_2(z)$, where f_1 and f_2 are entire functions of exponential type τ, real for real z, and bounded by 1 on the real axis. Since $\mathcal{L}(e^{i\theta}f) = e^{i\theta}\mathcal{L}(f)$, we can choose θ so that $\mathcal{L}(e^{i\theta}f) = |\mathcal{L}(f)|$, and so $\mathcal{L}(f_1) = |\mathcal{L}(f)|$. Hence the maximum of $|\mathcal{L}(f)|$ is attained, if at all, for an f which is real on the real axis, and for which $\mathcal{L}(f) \geqq 0$.

Let $\mathfrak{F}_\tau$ denote the class of entire functions f of exponential type τ which are real for real z and satisfy $|f(x)| \leqq 1$ for $-\infty < x < \infty$. (We emphasize that in our terminology $\mathfrak{F}_\tau$ includes all functions of order 1 and type not exceeding τ, as well as all entire functions of order less than 1.)

LEMMA 2.2. *If τ and a linear functional $\mathcal{L}$ are given then $M = \sup |\mathcal{L}(f)|$, $f \in \mathfrak{F}_\tau$, is finite, positive, and attained.*

It is well known (cf. [2], p. 83) that if $f \in \mathfrak{F}_\tau$ then

$$|f(x+iy)| \leqq e^{\tau|y|}, \tag{2.3}$$

so that $\mathfrak{F}_\tau$ is a normal family. Bernstein's theorem shows that M is finite, and so it is attained for some element of $\mathfrak{F}_\tau$. Finally, M is positive because we can readily exhibit elements of $\mathfrak{F}_\tau$ for which $f^{(j)}(x_\nu) = 0$ for all j and ν entering the definition of $\mathcal{L}$, except $\nu = m$, $j = n_m$. Indeed, we can have $\mathcal{L}(f) \neq 0$ for an f such that $f(x) \to 0$ as $|x| \to \infty$. To verify this, let $p(z)$ be a polynomial with real coefficients which has a zero of order n_1 at x_1 and zeros of order $n_\nu + 1$ at x_ν for $\nu \neq 1$, so that $p(z)$ is of degree $l-1$. Then

$$f(z) = c\{[\sin \epsilon(z - x_1)]/(z - x_1)\}^l p(z)$$

has the desired property if ϵ and c are small enough positive constants, since $f^{(k)}(z_\nu) = 0$ for $k = 0, 1, \cdots, n_\nu$ and $\nu = 2, 3, \cdots, m$, while $f^{(n_1)}(x_1) \neq 0$.

Our central result is as follows.

THEOREM 1. *The element f of $\mathfrak{F}_\tau$ for which*

$$\mathcal{L}(f) = \sup \mathcal{L}(g), \qquad g \in \mathfrak{F}_\tau, \tag{2.4}$$

is unique, and either constant[2] *or of order* 1 *and type τ (i.e., not of exponential type less than τ). If not constant, it satisfies a differential equation*

$$\{f'(z)\}^2/(1-\{f(z)\}^2) = \tau^2\{p(z)\}^2/q(z), \tag{2.5}$$

where $p(z)$ and $q(z)$ are monic polynomials with real coefficients; the degree of $p(z)$ is at most $l-2$ and the degree of $q(z)$ is precisely twice that of $p(z)$. The zeros of $q(z)$ are simple and not real, and $q(x) \geqq \{p(x)\}^2$ for real x, with equality at some point if and only if $p(z) \equiv q(z) \equiv 1$.

This result may be formulated in somewhat different language. If $x_1, \cdots, x_m$ are given distinct real numbers and $n_1, \cdots, n_m$ are nonnegative integers, then

$$(f(x_1), f'(x_1), \cdots, f^{(n_1)}(x_1), \cdots, f^{(n_m)}(x_m))$$

is a point in l-dimensional Euclidean space, and we say that this point belongs to $f(z)$. Let E be the set of points belonging to the elements of $\mathfrak{F}_\tau$. The content of Lemma 2.2 is that E is closed and bounded and contains a point other than the origin. Furthermore, E is convex since $\mathfrak{F}_\tau$ is convex. Theorem 1 shows that a boundary point of E belongs to a unique element of $\mathfrak{F}_\tau$ and this function satisfies (2.5).

When all the n_ν are zero in (2.1), so that

$$\mathcal{L}(f) = \sum_{\nu=1}^{m} \alpha_\nu f(x_\nu),$$

Theorem 1 fails, but similar results can be obtained; see Section 15.

3. Lemmas for Theorem 1. If $f(z) \in \mathfrak{F}_\tau$ the real zeros of $1-f(z)^2$ are of even order and the imaginary zeros occur in conjugate pairs. Let $\lambda_1, \lambda_2, \cdots$ be the distinct real points where $1-f(z)^2 = 0$. We wish to consider the imaginary zeros of $1-f(z)^2$ together with the real zeros whose orders exceed 2. These are the zeros of the entire function

$$(1-f(z)^2)/\{\prod(1-z/\lambda_n)^2 e^{2z/\lambda_n}\}, \tag{3.1}$$

[2] We do not know of any example in which the extremal function is constant, but since the possibility causes little difficulty in any particular case, we have not attempted to exclude it.

and there are either a nonnegative even number of them, or infinitely many. If some $\lambda_\nu = 0$, the denominator contains the term z^2 and the product extends over $n \neq \nu$.

LEMMA 3.2. *If* (3.1) *has at least* $2k$ *zeros then there is a function* $g(z)$ *in* $\mathfrak{F}_\tau$ *which has a zero at each* λ_n *and is such that* $x^k g(x)$ *is bounded for real* x.

The zeros of (3.1) are either real or occur in conjugate pairs. Let $p(z)$ be a polynomial of degree $2k$, with real coefficients, which is nonnegative for real z and whose zeros are among the zeros of (3.1). Then $F(z) = \{1 - f(z^2\}/p(z)$ is an entire function of exponential type 2τ, real and nonnegative for real z, and it has a zero of order at least 2 at each λ_ν. Furthermore, $F(x)$ is bounded for real x (indeed, it is $O(x^{-2k})$ as $|x| \to \infty$). Then if z_n are the zeros of $F(z)$, it follows ([2], p. 86) that $\sum |\Im(1/z_n)| < \infty$. This implies ([2], p. 125) that there is an entire function $\phi(z)$ of exponential type τ such that $F(z) = \phi(z)\{\phi(z^*)^*\}$, where the star denotes the complex conjugate. Then $\phi(x) = O(|x|^{-k})$ as $|x| \to \infty$ and $\phi(\lambda_\nu) = 0$. Finally, $g(z) = c\{\phi(z) + \phi(z^*)^*\}$ has all the properties stated in Lemma 3.2 if c is a sufficiently small positive constant.

LEMMA 3.3. *Let* f *be an element of* $\mathfrak{F}_\tau$, *not constant, satisfying* (2.4). *Then* $|f(x)| = 1$ *for at least one real* x; *and if* $F(z) \in \mathfrak{F}_\tau$ *and* F *has a zero at each of the distinct real points where* $f(x) = \pm 1$, *then* $\mathcal{L}(F) = 0$.

We shall prove the second part of Lemma 3.3 here only under the additional hypothesis

$$\lim_{x \to +\infty} F(x) = 0. \tag{3.4}$$

After obtaining more information about the extremal function $f(z)$ we shall prove the lemma in full generality.

Consider the function $g_\epsilon(z) = f(z) + \epsilon F(z)$, where ϵ is real. Then $g_\epsilon(z)$ is entire and of exponential type τ. We begin by showing that if $F(z)$ is any element of $\mathfrak{F}_\tau$ and

$$\sup_{-\infty < x < \infty} |f(x) + \epsilon F(x)| = 1 + o(\epsilon), \qquad \epsilon \to 0, \tag{3.5}$$

where ϵ is real, then $\mathcal{L}(F) = 0$. For, let $0 < \rho < 1$. According to (3.5), if $|\epsilon| < \epsilon_0(\rho)$, the function

$$\psi_\epsilon(z) = \{f(z) + \epsilon F(z)\}/\{1 + |\epsilon|\rho\}$$

belongs to $\mathfrak{F}_\tau$. If $\mathcal{L}(F) \neq 0$ then

$$\mathcal{L}(\psi_\epsilon) = \{\mathcal{L}(f) + \epsilon\mathcal{L}(F)\}/\{1 + |\epsilon|\rho\}.$$

Choose ρ so that $\rho\mathcal{L}(f) < |\mathcal{L}(F)|$, then ϵ so that $|\epsilon| < \epsilon_0(\rho)$ and so that $\epsilon\mathcal{L}(F) > 0$. We then have $\mathcal{L}(\psi_\epsilon) > \mathcal{L}(f)$, contradicting the maximizing property assumed for f. Hence $\mathcal{L}(F) = 0$.

To establish the first part of Lemma 3.3, suppose $|f(x)| < 1$ for all finite x. We can find an F in $\mathfrak{F}_\tau$ satisfying (3.4) and with $\mathcal{L}(F) \neq 0$ as in the proof of Lemma 2.2. Write $g_\epsilon(x) = f(x) + \epsilon F(x)$. Let δ be a positive number and let $x_0 = x_0(\delta)$ be so large that $|F(x)| \leqq \delta$ for $|x| \geqq x_0$. Then

$$|g_\epsilon(x)| \leqq 1 + \delta|\epsilon|, \qquad |x| \geqq x_0. \tag{3.6}$$

Since $|f(x)| < 1$ in $|x| \leqq x_0$ we have $|g_\epsilon(x)| < 1$ in $|x| \leqq x_0$ if ϵ is small enough, so the inequality in (3.6) holds for all x. Hence (3.5) holds and we infer that $\mathcal{L}(F) = 0$, a contradiction.

Now suppose that F satisfies (3.4) and has a zero at each of the distinct real points where $f(x) = \pm 1$. Since F satisfies (3.4) we have (3.6) again, and (3.5) follows unless $|f(x)| = 1$ at some point in $|x| \leqq x_0$. In the latter case there are only a finite number of such points. Let λ be one of these points. Then there is an interval I with center at λ such that

$$|f(x)| \leqq 1 - h(x-\lambda)^{2\mu}$$

in I, where $h > 0$ and μ is a positive integer. Since $F(\lambda) = 0$, Bernstein's theorem shows that $|F(x)| \leqq \tau|x-\lambda|$, so

$$|g_\epsilon(x)| \leqq 1 - h(x-\lambda)^{2\mu} + \epsilon\tau|x-\lambda|$$

in I. The maximum of the right-hand side does not exceed $1 + B\epsilon^{1+1/(2\mu-1)}$, where B depends only on h, τ and μ. Thus $|g_\epsilon(x)| \leqq 1 + o(\epsilon)$ in the intervals I, while $|g_\epsilon(x)| \leqq 1$ for small ϵ outside these intervals. These facts, together with (3.6), establish (3.5). This implies, as we saw, that $\mathcal{L}(F) = 0$. This establishes the second part of Lemma 3.3 under the hypothesis (3.4).

LEMMA 3.7. *Given a set of distinct real points $\lambda_1, \lambda_2, \cdots$, if there is an element $G(z)$ of $\mathfrak{F}_\tau$, not vanishing identically, such that $G(\lambda_\nu) = 0$ and $G(x) = O(|x|^{1-l})$ as $|x| \to \infty$, then there is an element $g(z)$ of $\mathfrak{F}_\tau$ such that $g(\lambda_\nu) = 0$ and $\mathcal{L}(g) \neq 0$. If $G(x) = O(|x|^{-l})$ as $|x| \to \infty$, then, in addition, $g(x) \to 0$ as $|x| \to \infty$.*

If $G(z)$ has a zero at any of the points x_ν, let $G_1(z) = G(z)/p_1(z)$, where $p_1(z)$ is a polynomial with real coefficients whose zeros are in the intersection of $\{x_\nu\}$ and $\{\lambda_\nu\}$. If $G(z)$ has no zero at any x_ν let $G_1(z) = G(z)$. Then $G_1(z)$ is an entire function which has zeros at the λ_ν which are not in $\{x_\nu\}$. We have assumed that some $n_\nu > 0$; suppose for definiteness that $n_1 > 0$. Let $p_2(z)$ be a polynomial with real coefficients which has a zero of order n_1 at x_1 and zeros of order $n_\nu + 1$ at x_ν for $\nu \neq 1$. Then $p_2(z)$ is of degree $l - 1$. Define $g(z) = cG_1(z)p_2(z)$, where c is a real constant, not 0, but so small that $g \in \mathfrak{F}_\tau$. Then $g^{(k)}(x_\nu) = 0$ for $k = 0, 1, 2, \cdots, n_\nu$ and $\nu = 2, 3, \cdots, m$. Hence $\mathfrak{L}(g) = \alpha_1^{(n_1)} g^{(n_1)}(x_1) \neq 0$. The hypothesis $G(x) = O(|x|^{1-l})$ makes $g(x)$ bounded; so $G(x) = O(|x|^{-l})$ makes $g(x) \to 0$ as $|x| \to \infty$.

The only place where we have used the fact that some $n_\nu > 0$ (i.e., that $\mathfrak{L}(f)$ actually involves derivatives) is in the last part of the proof of Lemma 3.7. If all n_ν are 0, $g(x_1) \neq 0$, and in case x_1 happens to be a λ_ν we cannot complete the proof. Indeed, if all n_ν are 0 and all x_ν are λ_ν's we cannot have g in $\mathfrak{F}_\tau$ such that $g(\lambda_\nu) = 0$ and $\mathfrak{L}(g) \neq 0$.

4. Proof of part of Theorem 1. We prove part of Theorem 1, and then use this part to prove Lemma 3.3 without the additional hypothesis (3.4). Then we shall use Lemma 3.3 to complete the proof of Theorem 1.

Let $f(z)$, not a constant, belong to $\mathfrak{F}_\tau$ and maximize $\mathfrak{L}$ in $\mathfrak{F}_\tau$. To show, first, that $f(z)$ is not of exponential type less than τ, suppose that it is of type $\gamma < \tau$. Let $0 < \epsilon < \tau - \gamma$ and define $\phi(z) = \{\sin \epsilon z\}/p(z)$, where $p(z)$ is a polynomial of degree l with real coefficients, whose zeros are among the zeros of $\sin \epsilon z$. If c is a sufficiently small positive number, $G(z) = cf'(z)\phi(z)$ belongs to $\mathfrak{F}_\tau$. If λ_ν are the distinct real points where $f(x) = \pm 1$ (there is at least one, by the part of Lemma 3.3 that has been established), Lemma 3.7 gives us a function g such that $g(\lambda_\nu) = 0$, $\mathfrak{L}(g) \neq 0$, and $g(x) \to 0$ as $|x| \to \infty$. The special case of Lemma 3.3 which has already been proved now shows that $\mathfrak{L}(g) = 0$, a contradiction. Hence f is not of type less than τ.

Again let f, not a constant, belong to $\mathfrak{F}_\tau$ and maximize $\mathfrak{L}$ in $\mathfrak{F}_\tau$. We know that $1 - f(x)^2$ has at least one real zero; let the distinct points where $f(x) = \pm 1$ be $\lambda_1, \lambda_2, \cdots$. Then $f'(\lambda_\nu) = 0$. We shall show that $1 - f(z)^2$ has at most $2l - 2$ zeros besides its double zeros at the λ_ν, and that $f'(z)$ has at most $l - 1$ zeros besides its simple zeros at the λ_ν.

For, suppose $1 - f(z)^2$ has $2l$ additional zeros. Then the function (3.1) has at least $2l$ zeros. Let $g(z)$ be the function constructed in Lemma

3.2 with $k=l$. By Lemma 3.7 there is a function $g_1(z)$ which belongs to $\mathfrak{F}_\tau$ and has the properties

$$g_1(\lambda_\nu)=0, \quad \mathfrak{L}(g_1)\neq 0, \quad g_1(x)\to 0 \text{ as } |x|\to\infty. \tag{4.1}$$

This contradicts Lemma 3.3.

If $f'(z)$ has at least l zeros besides simple zeros at the λ_ν, let l of them be divided out; that is, write $G(z)=f'(z)/p(z)$, where $p(z)$ is a polynomial of degree l with real coefficients, such that $G(z)\in\mathfrak{F}_\tau$, with $G(\lambda_\nu)=0$. By Lemma 3.7 there is a function $g_1(z)$ in $\mathfrak{F}_\tau$ with the properties (4.1). This again contradicts Lemma 3.3.

Thus there is a polynomial $P_1(z)$ of degree at most $2l-2$ such that $\{1-f(z)^2\}/P_1(z)$ has zeros of order 2 at each λ_ν, and no other zeros. There is also a polynomial $P_2(z)$ of degree at most $l-1$ such that $f'(z)/P_2(z)$ has simple zeros at each λ_ν, and no other zeros. Hence

$$\phi(z)=\{f'(z)^2/(1-f(z)^2)\}\cdot\{P_1(z)/P_2(z)^2\}$$

is an entire function with no zeros, taking real values on the real axis. It is of exponential type, as may be seen, for instance, from minimum modulus theorems ([2], p. 52). Hence $\phi(z)$ is of the form e^{az+b} with real a and b. Thus

$$f'(z)^2/P_2(z)^2=e^{az+b}(1-f(z)^2)/P_1(z).$$

The left-hand side is bounded on the real axis, and if $a\neq 0$ it must decrease exponentially either as $x\to+\infty$ or as $x\to-\infty$. This is impossible, since $f'(z)\not\equiv 0$ ([2], p. 69), so $a=0$.

We thus have

$$f'(z)^2/(1-f(z)^2)=\gamma p(z)^2/q(z), \tag{4.2}$$

where p is a polynomial of degree at most $l-1$ and q is a polynomial of degree at most $2l-2$, each with real coefficients and leading coefficient 1. We suppose that all common factors of p^2 and q have been cancelled. Since everything is real on the real axis and the left-hand side of (4.2) is positive, $\gamma>0$. Thus

$$f'(z)/\{1-f(z)^2\}^{\frac12}=\gamma^{\frac12}p(z)/\{q(z)\}^{\frac12}.$$

Integrating this, we have

$$f(z)=\sin\psi(z), \tag{4.3}$$

where

$$\psi(z)=\gamma^{\frac12}\int_0^z\{q(z)\}^{-\frac12}p(w)\,du+\sin^{-1}f(0). \tag{4.4}$$

Since $f(z)$ is not of exponential type less than τ, we see that the degree of q is precisely twice that of p, and that $\gamma^{\frac{1}{2}} = \pm \tau$.

Since the rational function in (4.2) is in lowest terms, $p(z_0) \neq 0$ if z_0 is at least a double zero of $q(z)$. It now follows that $q(z)$ has only simple zeros. For, if z_0 is at least a double zero of $q(z)$, then $p(z_0) \neq 0$, and (4.4) shows that $|\psi(z)| \to \infty$ as $z \to z_0$. But $f(z) = \sin \psi(z)$ is regular at z_0.

Hence $q(z)$ has no real zeros, since everything in (4.2), except possibly $q(z)$, is nonnegative for real z. Thus $q(x) \geqq 0$ and any real zeros of q would have to be multiple.

Our next task is to show that $p(z)$ is of degree at most $l-2$. This will follow from Lemma 3.3 without the additional hypothesis (3.4), so we now complete the proof of Lemma 3.3.

5. Completion of the proof of Lemma 3.3. Let f, not a constant, be an element of $\mathfrak{F}_\tau$ maximizing $\mathcal{L}(f)$ and let $F \in \mathfrak{F}_\tau$, with $F(\lambda_\nu) = 0$ for each λ_ν such that $f(\lambda_\nu) = \pm 1$. Define $g_\epsilon(z) = f(z) + \epsilon F(z)$ with ϵ real. Then $f(z) = \sin \psi(z)$ with $\psi(z)$ defined by (4.4). We can find a point x_1 such that

$$\tfrac{1}{2}\tau \leqq |\psi'(x)| \leqq 2\tau, \qquad |x| \geqq x_1 - 1/(2\tau). \tag{5.1}$$

If $\{\lambda_\nu\}$ are the points where $|f(x)| = 1$, we know that $f'(z)$ has at most $l-1$ zeros besides simple zeros at the λ_ν, so we can choose x_1 also so large that none of these $l-1$ zeros occurs in $|x| \geqq x_1 - 1/(2\tau)$. Finally let x_1 be such that $|f(\pm x_1)| < 1$. In $[-x_1, x_1]$ we have

$$\sup_{-x_1 \leqq x \leqq x_1} |g_\epsilon(x)| = 1 + o(\epsilon), \qquad \epsilon \to 0, \tag{5.2}$$

as was shown in the first part of the proof of Lemma 3.3 in Section 3.

Now consider a point λ_ν in $|x| > x_1$. Since $f(z) = \sin \psi(z)$ where $\psi(z)$ is given by (4.4), and the integrand in (4.4) tends to 1 as $x \to \pm\infty$ through real values, $\psi(x) \sim \tau x$ as $x \to \pm \infty$ and so there are an infinity of λ_ν in $x > x_1$ and in $x < -x_1$. In an interval $|x - \lambda_\nu| < 1/(2\tau)$ we have by (5.1)

$$|x - \lambda_\nu|\, \tau/2 \leqq |\psi(x) - \psi(\lambda_\nu)| \leqq 2\tau\, |x - \lambda_\nu| \leqq 1.$$

Since $\psi(\lambda_\nu) = (n + \frac{1}{2})\pi$ and $\cos\theta \leqq 1 - \theta^2/3$ for $-1 \leqq \theta \leqq 1$ this implies that

$$|f(x)| = |\cos\{\psi(x) - \psi(\lambda_\nu)\}| \leqq 1 - \tau^2 (x - \lambda_\nu)^2/12 \tag{5.3}$$

for $|x - \lambda_\nu| \leqq 1/(2\tau)$. In particular, at the end points of these intervals

we have $|f(x)| \leqq \frac{47}{48}$. Now $f'(x)$ has no zeros in the part of $|x| > x_1$ that lies outside these intervals, and so $f(x)$ is montonic in each of them; and there are λ_ν arbitrarily near $\pm\infty$. Hence $|f(x)| \leqq \delta < 1$ in the part of $|x| \geqq x_1$ that lies outside all the intervals, where δ is the maximum of $\frac{47}{48}$, $|f(\pm x_1)|$; so $|g_\epsilon(x)| \leqq 1$ outside these intervals if ϵ is small enough.

Now $|F(x)| \leqq \tau |x - \lambda_\nu|$ since $F(\lambda_\nu) = 0$ and $|F'(x)| \leqq \tau$ by Bernstein's theorem. Hence by (5.3) we have

$$|g_\epsilon(x)| \leqq 1 + 3\epsilon^2, \qquad |x - \lambda_\nu| \leqq 1/(2\tau),$$

if $|\epsilon|$ is sufficiently small. We thus have

$$\sup_{-\infty < x < \infty} |g_\epsilon(x)| = 1 + o(\epsilon), \qquad \epsilon \to 0.$$

This is (3.5), now without any auxiliary hypothesis on $F(z)$, and the proof of Lemma 3.3 can be completed as in Section 3.

6. Completion of the proof of Theorem 1. Now let f be an element of $\mathfrak{F}_\tau$, not a constant, maximizing $\mathfrak{L}(f)$. If λ_ν are the distinct real points where $f(x) = \pm 1$ we have shown that $f'(z)$ has at most $l - 1$ zeros besides simple zeros at the λ_ν. We now show that this number is actually at most $l - 2$. If it is $l - 1$, let $p_1(z)$ be a polynomial of degree $l - 1$, with real coefficients, having zeros at the $l - 1$ extra zeros of $f'(z)$, and consider $f'(z)/p_1(z)$. Taking this as the $G(z)$ of Lemma 3.7, we have an element g of $\mathfrak{F}_\tau$ such that $g(\lambda_\nu) = 0$ and $\mathfrak{L}(g) \neq 0$. But Lemma 3.3 says that $\mathfrak{L}(g) = 0$. This shows that the polynomial $p(z)$ of (2.5) is of degree at most $l - 2$.

We next show that the extremal function in Theorem 1 is unique. Suppose that f_1 and f_2 are two extremal functions, not constants, and consider $f(z) = \frac{1}{2}\{f_1(z) + f_2(z)\}$. Then $f \in \mathfrak{F}_\tau$ and f is also an extremal function. At each real point λ_ν where $f(x) = \pm 1$ we must have $f_1(\lambda_\nu) = f_2(\lambda_\nu) = f(\lambda_\nu) = \pm 1$ since $|f_1(x)| \leqq 1$ and $|f_2(x)| \leqq 1$. Thus $g(z) = f_1(z) - f_2(z)$ has a zero of order at least 2 at each λ_ν. Thus $g(z)$, a function of exponential type τ, has approximately as many zeros as the function $1 - f(z)^2$, which is of order 1 and type 2τ (i.e., not of type less than 2τ), and since most of the zeros of $1 - f(z)^2$ are real, this is impossible. More precisely, f is given by (4.3), where $\psi(x) \sim \tau x$ as $|x| \to \infty$, so the distance between consecutive λ_ν's must be $\pi/\tau + o(1)$ as $|\lambda_\nu| \to \infty$. If $n_\phi(x)$ denotes the number of zeros of the function ϕ in $|z| < x$, we have $n_g(x) \geqq n_h(x)$, $h = 1 - f^2$, and this exceeds $(4\tau/\pi) + o(1)$; while, since g is of the exponential type τ, we have from Carleman's theorem $n_g(x) \leqq (2\tau/\pi)x + o(1)$ (cf. [2], p. 155).

(It would be enough to use the fact ([2], p. 16) that by Jensen's theorem $n_g(x) \leqq \tau x + o(1)$ for an infinity of x tending to ∞.) This contradiction shows that $f_1(z) - f_2(z) \equiv 0$.

Now suppose that $f_1(z) \equiv 1$ and $f_2(z) \not\equiv 1$ are extremal functions. Then $f(z) = \frac{1}{2}\{f_1(z) + f_2(z)\}$ is another non-constant extremal function, which therefore has the form (4.4) and consequently takes negative values; but clearly $f(z) \geqq 0$. This contradiction shows that if an extremal function is constant, there is no other extremal function.

Now we complete the proof of Theorem 1 by showing that the polynomials $p(z)$ and $q(z)$ satisfy

$$(6.1) \qquad q(x) \geqq p(x)^2$$

on the real axis with equalty at some point if and only if p and q are both constant. For, since $f(z)$ belongs to $\mathfrak{F}_\tau$, by a sharpened form of Bernstein's theorem it satisfies ([2], p. 215) $\tau^2 f(x)^2 + f'(x)^2 \leqq \tau^2$, i.e. $\tau^2(1 - f(x)^2) \geqq f'(x)^2$ on the real axis, with equality at some point if and only if $f(x) = \sin(\tau z + \beta)$ for some real β. Combining this with (2.5) we have, at any point where $1 - f^2 \neq 0$, the inequality $p(x)^2/q(x) \leqq 1$, with equality if and only if $f(z) = \sin(\tau z + \beta)$; and in the latter case $p \equiv q \equiv 1$. There remains the possibility that $p(x)^2 = q(x)$ at a point x_1 where $f(x_1) = \pm 1$. In this case the left-hand side of (2.5) approaches $\pm f''(x_1)$ as $x \to x_1$. By Bernstein's theorem, $|f''(x)| < \tau^2$ unless $f(z) \equiv \sin(\tau z + \beta)$, and so again $p(x)^2 < q(x)$ unless $p \equiv q \equiv 1$.

7. Continuity of the extremal function. We make the following remark, which is useful in analyzing special cases of Theorem 1.

THEOREM 2. *Let $f_\tau(z)$ be the extremal function of Theorem 1. Then $\mathfrak{L}(f_\tau)$ and $f_\tau(z)$ are continuous functions of τ in $0 < \tau < \infty$.*

Suppose $\sigma > \tau$. Then $f_\tau(z) \in \mathfrak{F}_\tau \subset \mathfrak{F}_\sigma$, so $\mathfrak{L}(f_\tau) < \mathfrak{L}(f_\sigma)$. The inequality is strict since f_σ is unique and not of type less than σ. Thus $\mathfrak{L}(f_\tau)$ is a strictly increasing function of τ. To show that it is continuous it is then enough to show that

$$(7.1) \qquad \lim_{\sigma \downarrow \tau} \mathfrak{L}(f_\sigma) \leqq \mathfrak{L}(f_\tau).$$

Since $|f_\sigma(x + iy)| \leqq e^{\sigma|y|}$, as $\sigma \to \tau$ through any sequence of values there is a subsequence for which $f_\sigma(z) \to g(z)$, uniformly on compact sets. Then $g(z) \in \mathfrak{F}_\tau$, and since $f_\sigma^{(k)}(x_\nu) \to g^{(k)}(x_\nu)$ it follows that $\mathfrak{L}(f_\sigma) \to \mathfrak{L}(g) \leqq \mathfrak{L}(f_\tau)$. This shows that (7.1) is true.

Now again let $\sigma \to \tau$ through some sequence. Then there is a subsequence such that $f_\sigma(z) \to g(z) \in \mathfrak{F}_\tau$. Since $\mathcal{L}(g) = \lim_{\sigma\to\tau}\mathcal{L}(f_\sigma) = \mathcal{L}(f_\tau)$ and f_τ is unique, $g(z) = f_\tau(z)$.

8. A functional of order 3. The remainder of this paper is principally concerned with finding $A_n(\tau)$ in (1.1) for $n = 1$, when the relevant functional is of order 4. In principle this problem is solved by Theorem 1, but it is not possible to read off numerical results directly from that theorem.

First, however, we shall consider briefly some simpler cases, in particular, functionals of lower order. When $l = 2$, the general functional has the form $\mathcal{L}(f) = \lambda f(a) + \mu f'(a)$. Theorem 1 shows that the unique extremal is either constant or of the form $\sin(\tau z + \sin^{-1} f(0))$. The calculation of the maximum of $\mathcal{L}(f)$ is then elementary.

There are two essentially different types of functionals of order 3, namely

$$\lambda f(0) + \mu f(1) + \gamma f'(1) \tag{8.1}$$

and

$$\lambda f(0) + \mu f'(0) + \gamma f''(0). \tag{8.2}$$

In either case, Theorem 1 shows that the unique extremal is either constant or of the form

$$f(z) = \sin(\tau z + \sin^{-1} f(0)) \tag{8.3}$$

or

$$f(z) = \sin\psi(z), \tag{8.4}$$

$$\psi(z) = \pm\tau \int_0^z \{w-\beta)(w-\bar{\beta})\}^{-\frac{1}{2}}(w-a)\,dw + \sin^{-1} f(0),$$

where a is real and β is not real. Let $b = \Re(\beta)$.

The integral in (8.4) can be evaluated explicitly in terms of elementary functions, and we obtain

$$\begin{aligned}\psi(z) = \pm\tau\{&\surd(z^2 - 2bz + |\beta|^2) \\ &+ (b-a)\log(\surd(z^2-2bz+|\beta|^2) + z - b) \\ &- |\beta| - (b-a)\log(|\beta| - b)\} + \sin^{-1} f(0).\end{aligned}$$

If $\sin\psi(z)$ is to be entire, we must have $b - a = 0$ and so

$$\psi(z) = \pm\tau\{\surd(z^2 - 2bz + |\beta|^2) - |\beta|\} + \sin^{-1} f(0).$$

Thus either

$$\begin{aligned}f(z) = {}&\sin\tau\surd(z^2-2bz+|\beta|^2)\cos(\tau|\beta| - \sin^{-1} f(0)) \\ &- \cos\tau\surd(z^2-2bz+|\beta|^2)\sin(\tau|\beta| - \sin^{-1} f(0))\end{aligned}$$

or

$$f(z) = -\sin \tau\sqrt{(z^2 - 2bz + |\beta|^2)}\cos(\tau|\beta| + \sin^{-1} f(0))$$
$$+ \cos \tau\sqrt{(z^2 - 2bz + |\beta|^2)}\sin(\tau|\beta| + \sin^{-1} f(0)).$$

In either case f can be entire only if the first term on the right vanishes, so that $\tau|\beta| \pm \sin^{-1} f(0)$ must be an odd multiple of $\pi/2$, and then

$$f(z) = \pm \cos \tau\sqrt{(z^2 - 2bz + |\beta|^2)}. \tag{8.5}$$

We now consider the special case of (8.2) when $\mu = 0$, $\gamma > 0$. There is then no loss of generality from taking $\gamma = 1$, and it is convenient to change the notation and consider

$$\mathcal{L}(f) = \tau^2\lambda f(0) + f''(0). \tag{8.6}$$

Then the maximum of $\mathcal{L}(f)$ is attained either by a constant (± 1); a function of the form $\sin(\tau z + c)$, for which $\mathcal{L}(f) = \tau^2(\lambda - 1)\sin c$, whose maximum is $\tau^2|\lambda - 1|$; or by a function (8.5).

In the last case put $\beta = re^{i\phi}$. Then

$$\pm \tau^{-2}\mathcal{L}(f) = \lambda \cos \tau r - (\tau r)^{-1} \sin \tau r \tag{8.7}$$
$$+ ((\tau r)^{-1} \sin \tau r - \cos \tau r)\cos^2 \phi.$$

The maximum modulus of the right-hand side clearly occurs when $\cos^2 \phi = 0$ or 1. But for the extremal function, β is not real, so we have $\cos \phi = 0$. Thus the extremal function is either of the form (8.3) or of the form

$$f(z) = \pm \cos \tau\sqrt{(z^2 + r^2)} \tag{8.8}$$

with

$$\pm \tau^{-2}\mathcal{L}(f) = \lambda \cos \tau r - (\tau r)^{-1} \sin \tau r.$$

When $\lambda < 0$ the extremal function is given by (8.3). For, the maximum modulus of the right-hand side of (8.7) $(\cos \phi = 0)$ is at most $|\lambda| + 1$, and this is equal to $|\lambda - 1|$ if $\lambda \leqq 0$.

Also, if $f(z) \equiv -1$, $\mathcal{L}(f) = \tau^2|\lambda| < \tau^2|\lambda - 1|$.

If f is of the form (8.8), and so $\lambda > 0$, then if we set $\theta = \tau r$, we have

$$\mathcal{L}(f) = \tau^2 |\lambda \cos \theta - \theta^{-1} \sin \theta| \tag{8.9}$$

for some θ in $0 < \theta < \infty$; $\theta = 0$ is excluded since $r > 0$. In fact, $0 < \theta \leqq 2\pi$. For, if $\theta > 2\pi$ the uniqueness of the extremal function implies that $|\lambda \cos \theta - \theta^{-1} \sin \theta|$ must be decreased when θ is either increased or decreased by 2π. But this cannot be the case if $\theta > 2\pi$.

On the other hand, if $\lambda \geqq \frac{1}{2}$ the extremal function is of the form (8.8).

For, if $\theta=\pi$ then (8.9) shows that $\mathscr{L}(f)\geqq\tau^2\lambda$, and this is at least as large as $\tau^2|1-\lambda|$ when $\lambda\geqq\frac{1}{2}$.

THEOREM 3. *For $\lambda\leqq\frac{1}{3}$ the maximum of $\tau^2\lambda f(0)+f''(0)$ for $f\in\mathfrak{F}_\tau$ is $\tau^2(1-\lambda)$ and is attained for the function $f(z)=-\cos\tau z$. If $\lambda>\frac{1}{3}$ the extremal function f is of the form $\pm\cos\{\tau(z^2+r^2)^{\frac{1}{2}}\}$ and*

$$\mathscr{L}(f)=\tau^2\max_{0<\theta\leqq\pi}(\theta^{-1}\sin\theta-\lambda\cos\theta). \tag{8.10}$$

If the extremal function is of the form (8.8) then $\lambda>0$ and $\mathscr{L}(f)$ is given by (8.9) for some θ in $0<\theta\leqq 2\pi$. If $\pi<\theta\leqq 3\pi/2$, the value of $|\lambda\cos\theta-\theta^{-1}\sin\theta|$ is increased if we replace θ by $2\pi-\theta$. If $3\pi/2<\theta\leqq 2\pi$, the value of this same expression is not decreased if we replace θ by $\theta-\pi$. Thus θ lies in $0<\theta\leqq\pi$, as indicated in (8.10). Now $\mathscr{L}(f)>0$, so if $\tau^{-2}\mathscr{L}(f)=\lambda\cos\theta-\theta^{-1}\sin\theta$, then $\lambda\cos\theta>\theta^{-1}\sin\theta$ and θ lies in $0<\theta<\pi/2$. In this case $|\lambda\cos\theta-\theta^{-1}\sin\theta|$ is not decreased if we replace θ by $\pi-\theta$.

Thus if the extremal function is of the form (8.8) the maximum $\mathscr{L}(f)$ is given by (8.10), with $\lambda>0$, or is $\tau^2\lambda$, corresponding to $f(z)\equiv 1$. We can exclude the latter possibility, however, since when θ is near π, we have

$$\begin{aligned}\theta^{-1}\sin\theta-\lambda(1-\cos\theta)&=2\theta^{-1}\sin\tfrac{1}{2}\theta\cos\tfrac{1}{2}\theta-2\lambda\cos^2\tfrac{1}{2}\theta\\&=2\cos\tfrac{1}{2}\theta(\theta^{-1}\sin\theta-\lambda\cos\tfrac{1}{2}\theta)>0.\end{aligned}$$

The extremal function depends continuously on λ, since it is unique for each λ. If $\lambda\leqq 0$ the extremal function is of the form (8.3) and if $\lambda\leqq\frac{1}{2}$ it is of the form (8.8), so there must be a value of λ for which it changes from one form to the other. The change can occur only when $r=\theta/\tau=0$. Now

$$\theta^{-1}\sin\theta-\lambda\cos\theta=1-\lambda+\theta^2(\tfrac{1}{2}\lambda-\tfrac{1}{6})+\theta^4(-\tfrac{1}{24}\lambda+\tfrac{1}{120})-\cdots.$$

Thus $\theta^{-1}\sin\theta-\lambda\cos\theta$ takes values greater than $1-\lambda$ near $\theta=0$ if and only if $\lambda>\frac{1}{3}$, so for $\lambda>\frac{1}{3}$ the extremal function is of the form (8.8).

When $\lambda\leqq\frac{1}{3}$ the maximum of $\mathscr{L}(f)$ can also be obtained by using an interpolation series (as in [2], chapter 11):

$$\tau^{-2}\mathscr{L}(f)=(\lambda-\tfrac{1}{3})f(0)=4\pi^{-2}\sum_{n=1}^{\infty}(-1)^n n^{-2}f(n\pi/\tau).$$

For $\lambda>\frac{1}{3}$ we naturally cannot obtain the best inequality in this way.

9. The maximum of $f'(\frac{1}{2})-f'(-\frac{1}{2})$.

The functional

$$\mathscr{L}(f)=f'(\tfrac{1}{2})-f'(-\tfrac{1}{2}),$$

like $f'(\frac{1}{2})+f'(-\frac{1}{2})$, is of order 4, but it turns out to have a much simpler theory than $f'(\frac{1}{2})+f'(-\frac{1}{2})$, which we shall consider in Sections 10 ff. If $\mathcal{L}(f)$ attains its maximum for the function $f(z)$ in $\mathfrak{F}_\tau$, it also attains its maximum for the function $f(-z)$, and since the extremal function is unique this shows that f must be even. We showed in Section 6 that $f'(x)$ has at most two zeros ("extra zeros") besides simple zeros at the points where $f(x)=\pm 1$. There are two cases to consider: (i) $|f(0)|<1$; (ii) $f(0)=\pm 1$. In either case $f'(0)=0$ since f' is an odd function, and f' has a zero of odd order at 0. In case (i), f' cannot have three or more zeros at 0, so it has just one. If f' has any other extra zeros it has at least two (since it is odd), and so at least three extra zeros in all, which is impossible. Thus in case (i) f' has no extra zeros except at 0, and $p(z)=(z)$ in (4.2).

In case (ii), if f' has any real extra zeros except at 0, it has two between a maximum and a minimum of f and hence (since it is odd, and 0 is an extremum of f) it has four, which is impossible. If the extra zeros are all at 0, there is a triple zero there; in this case, $p(z)^2/q(z)$, when reduced to lowest terms, has only a double zero at 0, so again $p(z)=z$. Thus either $p(z)=z$ or $f'(z)$, if it has extra zeros, has a conjugate imaginary pair which must be pure imaginary, since otherwise since f' is odd) there would be four extra zeros. Thus $f'(\pm ic)=0$, $c>0$. Consider the function

$$g(z)=\epsilon f'(z)(z^2+c^2)^{-1}(z^2-\tfrac{1}{4}),$$

where ϵ is real. Then $g\in\mathfrak{F}_\tau$ if $|\epsilon|$ is small enough, $g(\lambda)=0$ for every real zero λ of $1-f^2$, and (since g is odd) $\mathcal{L}(g)=2g'(\frac{1}{2})=2\epsilon f'(\frac{1}{2})/(\frac{1}{4}+c^2)$ $\neq 0$, since if $f'(\frac{1}{2})=0$ and f' is odd, f is certainly not an extremal function. But this contradicts Lemma 10.3. Hence f' has no extra zeros in case (ii).

Thus either $f(z)=\pm\cos\tau z$, corresponding to $p(z)=1$, or $f(z)=\sin\psi(z)$ with $\psi(z)$ given by (4.4) and $p(w)=w$. In the second case,

$$q(x)=x^2+ax+b>p(x)^2$$

for all real x, and so $a=0$ and $b>0$. Thus if $f(z)\neq\pm\cos\tau z$, we have

$$f(z)=\pm\sin\{\tau\int_0^z(x^2+c^2)^{-\frac{1}{2}}x\,dx+\lambda\}=\pm\sin\{\tau[(z^2+c^2)^{\frac{1}{2}}-c]+\lambda\}.$$

Since $f(z)$ is entire, we must then have $\lambda-c\tau=(2k+1)\pi/2$, and so

$$f(z)=\pm\cos\tau(z^2+c^2)^{\frac{1}{2}}. \tag{9.1}$$

If $f(z)=\pm\cos\tau z$ we have

$$\mathcal{L}(f)=2f'(\tfrac{1}{2})=\pm 2\tau\sin\tfrac{1}{2}\tau.$$

If $f(z)$ is given by (9.1), we have

$$\mathcal{L}(f) = \pm 2\tau\{\sin\tau(\tfrac{1}{4}+c^2)^{\frac{1}{2}}\}/\{2(\tfrac{1}{4}+c^2)^{\frac{1}{2}}\}.$$

Hence the maximum of $\mathcal{L}(f)$ is the larger of

$$(9.2) \qquad 2\tau\,|\sin\tfrac{1}{2}\tau\,|, \qquad 2\tau\,|\{\sin\tau(\tfrac{1}{4}+c^2)^{\frac{1}{2}}\}/\{2(\tfrac{1}{4}+c^2)^{\frac{1}{2}}\}|, \qquad c>0.$$

Clearly, if $\tau=2k\pi$ $(k=1,2,\cdots)$ the first expression in (9.2) is zero and the extremal function must be of the form (9.1); while if $\tau=(2k+1)\pi$, the first is 2τ, the maximum permitted by Bernstein's theorem, so the extremal function must be $\pm\cos\tau z$. A complete solution of our problem is given by the following theorem.

THEOREM 4. *Let* t_n $(n=1,2,\cdots)$ *be the root of* $\tan x = x$ *in* $(n\pi,(n+1)\pi)$, *and let* s_n *be the point in* $(n-1)\pi<x<n\pi$ *where* $|\sin s_n|/s_n = |\sin t_n|/t_n$. *Then the function in* $\mathfrak{F}_\tau$ *maximizing* $f'(\frac{1}{2}) - f(-\frac{1}{2})$ *is* $\pm\cos\tau z$ *for* τ *in the intervals* $(0,2s_1),(2t_1,2s_2),\cdots$; *for* τ *in the intervals* $(2s_1,2t_1),(2s_2,2t_2),\cdots$, *it is of the form* (9.1), *and the maximum of* $\mathcal{L}(f)$ *is* $\tau^2|\sin t_n|/t_n$ *if* $2s_n<\tau<2t_n$.

Write $\sigma=\frac{1}{2}\tau$ and $u^2=1+4c^2>1$. Then the extremal function is of the form (9.1) if and only if the second quantity in (9.2) is larger than the first, i. e.,

$$(9.3) \qquad (\sigma u)^{-2}\sin^2\sigma u > \sigma^{-2}\sin^2\sigma.$$

Now the graph of the function $\sigma^{-2}\sin^2\sigma$ consists of a series of arches of decreasing height, with maxima at the points 0, t_n $(n\geqq 1)$. There is a $u>1$ for which (9.3) holds if and only if σ is in the intervals (s_n,t_n) (F. Riesz's "rising sun" lemma), and the largest value of $|\sin u|/(\sigma u)$ is the value of $|\sin\sigma|/\sigma$ at t_n.

10. The maximum of $f'(\frac{1}{2})+f'(-\frac{1}{2})$. We now consider the case $n=1$ of (1.1). To obtain a symmetric result, let us put $x=-\frac{1}{2}$ and ask for the maximum of

$$(10.1) \qquad f'(\tfrac{1}{2})+f'(-\tfrac{1}{2})$$

when $f(z)$ is an entire function of exponential type τ with $|f(x)|\leqq 1$ for real x. As we showed in Section 2, there is no loss of generality in taking $f(z)$ real on the real axis, so we may assume that $f\in\mathfrak{F}_\tau$. Then (10.1) is a linear functional of order $l=4$. There is, by Theorem 1, a function f for which (10.1) attains its maximum. Then (10.1) also attains its maximum for the function $-f(-z)$, and since the extremal function is

unique this shows that $f(z)$ is an odd function. Hence from Theorem 1 we have

$$f(z) = \sin \psi(z), \tag{10.2}$$

where

$$\psi(z) = \tau\delta \int_0^z \{q(w)\}^{-\frac{1}{2}} p(w)\,dw, \qquad \delta = \pm 1, \tag{10.3}$$

$p(z)$ and $q(z)$ are monic, with real coefficients, and even, with $p(z)$ either constant or of degree 2, and $q(z)$ of twice the degree of $p(z)$ and with no real roots. We take the square root which is positive for real w. For real z we may take the path of integration along the real axis. Then

$$\mathcal{L}(f) = f'(\tfrac{1}{2}) + f'(-\tfrac{1}{2}) = 2\psi'(\tfrac{1}{2}) \cos \psi(\tfrac{1}{2}). \tag{10.4}$$

If $p(w)$ is constant, so is $q(w)$, and then

$$f(z) = \delta \sin \tau z, \qquad \mathcal{L}(f) = 2\delta\tau \cos \tfrac{1}{2}\tau.$$

By Bernstein's theorem we have $|f'(x)| \leqq \tau$ for all real x, so if n is a positive integer and $\tau = 2n\pi$, the function $(-1)^n \sin 2n\pi z$ is the extremal function for (10.1).

If $p(w)$ is not constant, it is of degree 2 and $q(w)$ is of degree 4. We can then write

$$\begin{aligned} p(w)/\{q(w)\}^{\frac{1}{2}} &= (w^2 + \alpha)/\{(w^2 - w_1^2)(w^2 - \bar{w}_1^2)\}^{\frac{1}{2}} \\ &= (w^2 + \alpha)/\{w^4 - 2w^2 r^2 \cos 2\theta + r^4\}^{\frac{1}{2}}, \end{aligned} \tag{10.5}$$

where α is real and $w_1 = re^{i\theta}$, $0 < \theta < \pi/2$.

We first find restrictions imposed on the parameters by the fact that $f(z)$ is entire. Near a zero w_1 of $q(w)$ we see that

$$\psi(z) = \psi(w_1) + (z - w_1)^{\frac{1}{2}} g(z),$$

where $g(z)$ is regular in a neighborhood of w_1. Now

$$\sin \psi(z) = \sin \psi(w_1) \cos \{(z - w_1)^{\frac{1}{2}} g(z)\} + \cos \psi(w_1) \sin \{(z - w_1)^{\frac{1}{2}} g(z)\},$$

so that for $\sin \psi(z)$ to be single-valued we must have $\cos \psi(w_1) = 0$. We can accordingly write

$$\psi(w_1) = \delta(m - \tfrac{1}{2})\pi, \tag{10.6}$$

where m is an integer and δ is the same as in (10.3). (We introduce δ here only to simplify the appearance of later formulas.)

To calculate $\psi(w_1)$ we take as the path of integration the segment of

the real axis from $z=0$ to $z=r$ together with the circular arc $w=re^{i\phi}$, $0\leqq\phi\leqq\theta$. Then

$$\psi(w_1)=\tau\delta\int_0^r(x^4-2x^2r^2\cos 2\theta+r^4)^{-\frac{1}{2}}(x^2+\alpha)\,dx$$
$$+\{i\tau\delta/(2r)\}\int_0^\theta(\sin^2\theta-\sin^2\phi)^{-\frac{1}{2}}(r^2e^{2i\phi}+\alpha)\,d\phi.$$

If we put $x=rt$ in the first integral and then take real and imaginary parts (using (10.6)) we find

$$\int_0^\theta(\sin^2\theta-\sin^2\phi)^{-\frac{1}{2}}(\alpha+r^2\cos 2\phi)\,d\phi=0, \tag{10.7}$$

$$(10.8)\quad (m-\tfrac{1}{2})\pi/(\tau r)=\int_0^1(t^4-2t^2\cos 2\theta+1)^{-\frac{1}{2}}(t^2+\alpha/r^2)\,dt$$
$$-\tfrac{1}{2}\int_0^\theta(\sin^2\theta-\sin^2\phi)^{-\frac{1}{2}}\sin 2\phi\,d\phi$$
$$=\int_0^1(t^4-2t^2\cos 2\theta+1)^{-\frac{1}{2}}(t^2+\alpha/r^2)\,dt-\sin\theta.$$

Conversely, if (10.7) and (10.8) are satisfied then if $\psi(z)$ is defined by (10.3), (10.5), the function $f(z)=\sin\psi(z)$ belongs to $\mathfrak{F}_\tau$.

In the next section we shall find a simpler version of the relations among the parameters α, θ, and r implied by (10.5), (10.6). First, however, we shall state our results.

For $n=0,1,2,\cdots$ let χ_n, γ_n be the unique numbers defined by

$$\tfrac{1}{2}\chi_n\tan\tfrac{1}{2}\chi_n=1,\qquad 2n\pi<\chi_n<(2n+1)\pi,$$
$$\gamma_0=\pi,\qquad \tfrac{1}{2}\gamma_n\tan\tfrac{1}{2}\gamma_n=-(\gamma_n^2+\pi^2)/(\gamma_n^2-\pi^2),$$
$$(2n+1)\pi<\gamma_n<(2n+2)\pi,\qquad n\geqq 1.$$

We append a short table of χ_n and γ_n, which was computed for us by Marilyn J. Woodyard.

n	0	1	2	3	4	5
$2n\pi$	0	6.28	12.57	18.85	25.13	31.42
χ_n	1.72	6.85	12.87	19.06	25.29	31.54
$(2n+1)\pi$	3.14	9.42	15.71	21.99	28.37	34.56
γ_n	3.14	12.19	18.62	24.97	31.29	37.59

THEOREM 5. *The extremal function* $f(z)$ *in* $\mathfrak{F}_\tau$ *for* $\mathfrak{L}(f)=f'(\frac{1}{2})+f'(-\frac{1}{2})$ *is* $\sin\tau z$ *in the interval* $0<\tau\leqq\chi_0$; *in the intervals* $\gamma_n\leqq\tau\leqq\chi_{n+1}$,

it is $(-1)^{n+1}\sin\tau z$. *In* $\chi_n < \tau < \gamma_n$, *it is* $\sin\psi(z)$, *where* $\psi(z)$ *is defined by* (10.3), (10.4), *the parameters satisfy* (10.5), (10.6), *with* $m = 0$, *and* $\delta = \pm 1$ *is chosen to make* $f'(\tfrac{1}{2}) > 0$.

More explicitly, the extremal function in $\chi_n < \tau < \gamma_n$ is $\sin\psi(z)$, where

$$\psi(z) = \pm\int_0^{\tau z}\{u^4 - 2u^2\boldsymbol{K}^2\cos 2\theta + \boldsymbol{K}^4\}^{-\frac{1}{2}}\{u^2 + \boldsymbol{K}(\boldsymbol{K} - 2\boldsymbol{E})\}\,du,$$

$\boldsymbol{K}$ and $\boldsymbol{E}$ are complete elliptic integrals of argument $\cos\theta$, and $0 < \theta < \pi/2$.

11. Relations among parameters. The integral in (10.7) can be conveniently expressed in terms of complete elliptic integrals. We can write it as

$$\begin{aligned}(1/\sin\theta)\int_0^{\theta}(1 - \csc^2\theta\sin^2\phi)^{-\frac{1}{2}}(\alpha + r^2(1 - 2\sin^2\phi))\,d\phi \\ = \csc\theta\{(\alpha + r^2\csc 2\theta)F(\theta,\csc\theta) + 2r^2\sin^2\theta E(\theta,\csc\theta)\} \\ = (\alpha - r^2)F(\pi/2,\sin\theta) + 2r^2E(\pi/2,\sin\theta) \\ = (\alpha - r^2)\boldsymbol{K}(\sin\theta) + 2r^2\boldsymbol{E}(\sin\theta),\end{aligned}$$

in the usual notation for elliptic integrals, so that (10.7) states that

$$(11.1)\qquad (\alpha - r^2)\boldsymbol{K}(\sin\theta) + 2r^2\boldsymbol{E}(\sin\theta) = 0.$$

Alternatively, we can calculate $\psi(w_1)$ by taking the path of integration along the imaginary axis from 0 to ir and along the arc $w = re^{i\phi}$, $\pi/2 \geqq \phi \geqq \theta$. Then we obtain

$$\begin{aligned}\psi(w_1) = i\tau\delta\int_0^{r}\{y^4 + 2y^2r^2\cos 2\theta + r^4\}^{-\frac{1}{2}}(-y^2 + \alpha)\,dy \\ - i\tau\delta/(2r)\int_{\theta}^{\pi/2}(\sin^2\phi - \sin^2\theta)^{-\frac{1}{2}}(r^2e^{2i\phi} + \alpha)\,d\phi.\end{aligned}$$

Taking real parts and using (10.4), we now find

$$\int_{\theta}^{\pi/2}(\sin^2\phi - \sin^2\theta)^{-\frac{1}{2}}(r^2\cos 2\phi + \alpha) = -(2m - 1)\pi/(\tau r).$$

This leads to

$$(11.2)\qquad (\alpha + r^2)\boldsymbol{K}(\cos\theta) - 2r^2\boldsymbol{E}(\cos\theta) = -(2m - 1)\pi r/\tau.$$

We may abbreviate (11.1), (11.2) in the usual notation as

$$\begin{aligned}&(\alpha - r^2)\boldsymbol{K} + 2r^2\boldsymbol{E} = 0,\\ &(\alpha + r^2)\boldsymbol{K}' - 2r^2\boldsymbol{E}' = pr, \qquad\qquad p = -(2m - 1)\pi/\tau.\end{aligned}$$

Solving for α and r, we find, using Legendre's relation $\boldsymbol{EK'}+\boldsymbol{E'K}-\boldsymbol{KK'}=\pi/2$,

$$(11.4)\qquad r=p\boldsymbol{K}/\pi,\qquad \alpha=r^2(\boldsymbol{K}-2\boldsymbol{E})/\boldsymbol{K}=p^2\boldsymbol{K}(\boldsymbol{K}-2\boldsymbol{E})/\pi^2.$$

It follows that r and α are continuous functions of θ for $0<\theta<\pi/2$, since $\boldsymbol{K}>0$ in this range.

We require a number of lemmas.

LEMMA 11.5. *As* $\theta\to 0$,

$$(11.6)\qquad \alpha/r^2=-1+\theta^2+O(\theta^4),$$

$$(11.7)\qquad (m-\tfrac{1}{2})\pi/(\tau r)=-1+\tfrac{1}{4}\theta^2+O(\theta^4).$$

If $\theta\to 0$ *and* $r\geqq\rho>\frac{1}{2}$, *then*

$$(11.8)\qquad p(w)/\{q(w)\}^{\frac{1}{2}}=-1+\{r^2(r^2+w^2)/(r^2-w^2)^2\}\theta^2+O(\theta^4),$$

uniformly in $0\leqq w\leqq\frac{1}{2}$.

From (11.4) we have $\alpha/r^2=(\boldsymbol{K}-2\boldsymbol{E})/\boldsymbol{K}$, and (11.6) follows from the expansions ([5], p. 3)

$$(11.9)\quad \boldsymbol{K}=\tfrac{1}{2}\pi(1+\tfrac{1}{4}\sin^2\theta+O(\sin^4\theta)),\quad \boldsymbol{E}=\tfrac{1}{2}\pi(1-\tfrac{1}{4}\sin^2\theta+O(\sin^4\theta)).$$

We also have $(m-\frac{1}{2})\pi/(\tau r)=-p/(2r)=-\pi/(2\boldsymbol{K})$, and (11.7) follows from (11.9).

To obtain (11.8), write

$$p(w)/\{q(w)\}^{\frac{1}{2}}=\{(w^2+\alpha)/(r^2-w^2)\}\{1+[4r^2w^2/(r^2-w^2)^2]\sin^2\theta\}^{-\frac{1}{2}}.$$

By (11.6), this is

$$\{-1+r^2\theta/(r^2-w^2)+O(\theta^4)\}\{1-2r^2w^2\theta^2/(r^2-w^2)^2+O(\theta^4)\}$$

and (11.8) follows.

LEMMA 11.10. *As* $\theta\to\pi/2$, *if* $s=\pi/2-\theta$ *we have*

$$(11.11)\qquad \alpha/r^2=1-2/\log(4/s)+O(s),$$

$$(11.12)\qquad (m-\tfrac{1}{2})\pi/(\tau r)=-\tfrac{1}{2}\pi/\log(4/s)+O(s),$$

and

$$(11.13)\qquad p(w)/\{q(w)\}^{\frac{1}{2}}=1-\{2/\log(4/s)\}\{r^2/(r^2+w^2)\}+O(s),$$

uniformly in $0\leqq w\leqq\frac{1}{2}$.

Here we use (11.4) and the expansions ([5], p. 3)

$$\begin{aligned} \boldsymbol{K} &= \log(4/\cos\theta) + \tfrac{1}{4}\{\log(4/\cos\theta) - 1\}\cos^2\theta \\ &\quad + O\{|\log|\cos\theta||\cdot\cos^4\theta\}, \\ \boldsymbol{E} &= 1 + \tfrac{1}{2}\{\log(4/\cos\theta) - \tfrac{1}{2}\}\cos^2\theta + O\{|\log|\cos\theta||\cdot\cos^4\theta\}. \end{aligned} \tag{11.14}$$

12. Estimates of $\sin\psi(z)$. In this section we consider a function, not necessarily extremal, of the form $f(z) = \sin\psi(z)$, where $\psi(z)$ is defined by (10.3), (10.5), the parameters satisfy (10.7) and (10.8), and δ is the same as in (10.3). We shall obtain several estimates for $f'(\tfrac{1}{2})$; the error terms are independent of m and τ over any bounded range of τ.

LEMMA 12.1. *If $\theta \to 0$ and $r \geqq \rho > \tfrac{1}{2}$ then*

$$-\delta f'(\tfrac{1}{2}) = \tau\cos\tfrac{1}{2}\tau + \tau\theta^2\{\tau G(r)\sin\tfrac{1}{2}\tau - H(r,\tfrac{1}{2})\cos\tfrac{1}{2}\tau\} + O(\theta^4),$$

where

$$H(r,w) = r^2(r^2+w^2)/(r^2-w^2)^2, \qquad G(r) = \int_0^{\frac{1}{2}} H(r,w)\,dw.$$

For, by Lemma 11.5,

$$\psi(\tfrac{1}{2}) = \delta\{-\tfrac{1}{2}\tau + \tau G(r)\theta^2 + O(\theta^4\},$$

whence

$$\cos\psi(\tfrac{1}{2}) = \cos\tfrac{1}{2}\tau + \tau G(r)\theta^2\sin\tfrac{1}{2}\tau + O(\theta^4);$$

and

$$\psi'(\tfrac{1}{2}) = \delta\tau\{-1 + H(r,\tfrac{1}{2})\theta^2 + O(\theta^4)\}.$$

Finally $f'(\tfrac{1}{2}) = \psi'(\tfrac{1}{2})\cos\psi(\tfrac{1}{2})$, and the conclusion follows.

LEMMA 12.2. *If $\theta \to \pi/2$ then*

$$\delta f'(\tfrac{1}{2}) = \tau\cos\tfrac{1}{2}\tau + \epsilon\tau(\tfrac{1}{2}\tau\sin\tfrac{1}{2}\tau - \cos\tfrac{1}{2}\tau) + O(\epsilon^2),$$

where

$$\epsilon = 1/\log\{4/(\tfrac{1}{2}\pi - \theta)\}.$$

This follows in the same way from Lemma 11.10.

LEMMA 12.3. *If $\theta \to 0$ and $r \to r_0$, where $0 < r_0 < \tfrac{1}{2}$, then*

$$\begin{aligned} \delta f'(\tfrac{1}{2}) = \tau\cos\tfrac{1}{2}\tau - \{2\theta^2\tau r_0^2/(1-4r_0^2)\}\{\tau\sin\tfrac{1}{2}\tau \\ + 2(1+4r_0^2)(1-4r_0^2)^{-1}\cos\tfrac{1}{2}\tau\} + O(\theta^2). \end{aligned}$$

For, by Lemma 11.5,

$$\delta\psi(\tfrac{1}{2})/(\tau r) = \int_0^{1/(2r)} \{(t^2-\cos 2\theta)^2 + \sin^2 2\theta\}^{-\frac{1}{2}}(t^2 - 1 + \theta^2 + O(\theta^4))\,dt.$$

We make the substitution $t^2 + \cos 2\theta = u \sin 2\theta$ over the part of the interval of integration where $-\theta^{-\frac{1}{2}} < u < \theta^{-\frac{1}{2}}$, that is, over $t_1 < t < t_2$ where

$$t_1 = \{\cos 2\theta - \theta^{-\frac{1}{2}} \sin 2\theta\}^{\frac{1}{2}} = 1 - \theta^{\frac{1}{2}} - \tfrac{1}{2}\theta - \tfrac{1}{2}\theta^{\frac{3}{2}} - \tfrac{13}{8}\theta^2 + O(\theta^{\frac{5}{2}}),$$

$$t_2 = \{\cos 2\theta + \theta^{-\frac{1}{2}} \sin 2\theta\}^{\frac{1}{2}} = 1 + \theta^{\frac{1}{2}} - \tfrac{1}{2}\theta + \tfrac{1}{2}\theta^{\frac{3}{2}} - \tfrac{13}{8}\theta^2 + O(\theta^{\frac{5}{2}}).$$

The integral defining $\psi(\frac{1}{2})$ will be written as the sum of integrals over the intervals $(0, t_1)$, (t_1, t_2), $(t_2, \frac{1}{2}r^{-1})$.

The integral over (t_1, t_2) is equal to

$$\tfrac{1}{2}\int_{-\theta^{-\frac{1}{2}}}^{\theta^{-\frac{1}{2}}} (u \sin 2\theta - \theta^2 + O(\theta^4))/\{(u^2+1)^{\frac{1}{2}}(\cos\theta + u \sin 2\theta)\} du$$

$$= \tfrac{1}{2}(\sec 2\theta)^{\frac{1}{2}} \int_{-\theta^{-\frac{1}{2}}}^{\theta^{-\frac{1}{2}}} \{(u \sin\theta - \theta^2 + O(\theta^4))/(u^2+1)^{\frac{1}{2}}\}$$
$$\times\{1 - \tfrac{1}{2}u \tan 2\theta + \tfrac{3}{8}u^2 \tan^2 2\theta - \tfrac{5}{16}u^3 \tan^3 2\theta$$
$$+ \tfrac{35}{128}u^4 \tan^4 2\theta + O(u^5\theta^5\} du.$$

Collecting the even part of the integrand, we see that this integral is equal to

$$-(\sec 2\theta)^{\frac{1}{2}} \int_0^{\theta^{-\frac{1}{2}}} (2u^2\theta^2 + 5u^4\theta^4 + \theta^2)(u^2+1)^{-\frac{1}{2}} du + O(\theta^3)$$
$$= -\theta - \tfrac{7}{4}\theta^2 + O(\theta^3).$$

The integral over $(0, t_1)$ is

$$\int_0^{t_1} [\{t^2 - 1 + \theta^2 + O(\theta^4)\}/(1-t^2)]\{1 + 4t^2 \sin^2\theta(1-t^2)^{-2}\}^{-\frac{1}{2}} dt$$
$$= \int_0^{t_1} \{-1 + [\theta^2 + O(\theta^4)]/(1-t^2)\}\{1 - 2t^2(1-t^2)^{-2}\sin^2\theta$$
$$+ O(\theta^4/(1-t)^4)\} dt$$
$$= \int_0^{t_1} \{-1 + (1+t^2)(1-t^2)^{-2}\theta^2\} dt + O(\theta^{\frac{5}{2}})$$
$$= -t_1 + \tfrac{1}{2}\theta^2\{1/(1-t_1) - 1/(1+t_1)\} + O(\theta^{\frac{5}{2}}).$$

The integral over $(t_2, 1/(2r))$ is

$$\int_{t_2}^{1/(2r)} \{(t^2 - 1 + \theta^2 + O(\theta^4))/(t^2-1)\}\{1 + 4t^2(t^2-1)^{-2}\sin^2\theta\}^{-\frac{1}{2}} dt$$
$$= \int_{t_2}^{1/(2r)} \{1 - (1+t^2)/(1-t^2)^{-2}\theta^2\} dt + O(\theta^{\frac{5}{2}})$$
$$= 1/(2r) - t_2 + \tfrac{1}{2}\theta^2\{1/(1-t_2) + 1/(1+t_2)\} - 2r\theta^2/(4r^2-1)$$
$$+ O(\theta^{\frac{5}{2}}).$$

Adding these results we obtain

$$\delta\psi(\tfrac{1}{2})/(\tau r) = 1/(2r) - 2 + \theta^2\{\tfrac{1}{2} - 2r/(4r^2 - 1)\} + O(\theta^{\frac{5}{2}}).$$

Then, referring to Lemma 11.5, we see that

$$r = r_0(1 + \tfrac{1}{4}\theta^2 + O(\theta^{\frac{5}{2}})), \qquad r_0 = (\tfrac{1}{2} - m)\pi/\tau.$$

Thus

$$\delta\psi(\tfrac{1}{2}) = \tfrac{1}{2}\tau - \theta^2 2\tau r_0/(4r_0^2 - 1) + o(\theta^2),$$

so that

$$\cos\psi(\tfrac{1}{2}) = \cos\tfrac{1}{2}\tau - \theta^2 2\tau r_0(1 - 4r_0^2)^{-1}\sin\tfrac{1}{2}\tau + o(\theta^2).$$

Since the limit of r is less than $\frac{1}{2}$ we have

$$\delta\psi'(\tfrac{1}{2}) = \tau - \theta^2\tau 4r_0^2(1 - 4r_0^2)/(1 - 4r_0^2)^2 + o(\theta^2),$$

and the lemma follows.

13. The case of small τ. We now turn to the proof of the results stated in Theorem 5. In this section we prove that for all small positive τ the extremal function is $f_\tau(z) = \sin\tau z$. We shall sometimes write $\psi_\tau(z)$ instead of $\psi(z)$ since the parameters α, r, θ, δ of the extremal function depend on τ.

Let $0 < \tau < \pi$. As we showed in Section 10, the element of $\mathcal{J}_\tau$ which maximizes $\mathcal{L}(f)$ is either $f_\tau(z) = \sin\tau z$ or $f_\tau(z) = \sin\psi_\tau(z)$, where $\psi_\tau(z)$ is defined by (10.3), (10.5). The case $f_\tau(z) = -\sin\tau z$ is excluded since $\mathcal{L}(f) > 0$.

The proof that the extremal function is $\sin\tau z$ for all small τ is by contradiction. Suppose that for a sequence of values of τ approaching 0 the extremal function is $f_\tau(z) = \sin\psi_\tau(z)$. Then

$$\psi_\tau'(\tfrac{1}{2})\cos\psi_\tau(\tfrac{1}{2}) > \tau\cos\tfrac{1}{2}\tau.$$

Now $q(w) \geqq p(w)^2$ for real w, so $\cos\psi_\tau(\frac{1}{2}) \to 1$, $\cos\frac{1}{2}\tau \to 1$ as $\tau \to 0$. Also

$$\psi_\tau'(\tfrac{1}{2}) = \tau p_\tau(\tfrac{1}{2})/\{q_\tau(\tfrac{1}{2})\}^{\frac{1}{2}} \leqq \tau,$$

so it follows that

$$p_\tau(\tfrac{1}{2})/\{q_\tau(\tfrac{1}{2})\}^{\frac{1}{2}} \to 1, \qquad \tau \to 0. \tag{13.1}$$

There is a subsequence of values of τ approaching zero such that $\theta \to \theta_0$, $0 \leqq \theta_0 < \pi/2$, and r approaches a limit, finite or infinite. There are several cases to consider.

If $0 < \theta_0 < \pi/2$ then, by (10.7) or (11.4), $\alpha/r^2 \to A$, where $-1 < A < 1$.

But the right-hand side of (10.8) approaches a finite limit as $\theta \to \theta_0$, so (10.8) shows that $r \to \infty$. Then from (10.5) we have

$$|\lim p_\tau(\tfrac{1}{2})/\{q_\tau(\tfrac{1}{2})\}^{\frac{1}{2}}| = |\lim \alpha/r^2| = |A| < 1,$$

and this contradicts (10.1).

If $\theta_0 = 0$, then Lemma 11.5 shows that $r \to \infty$. In Lemma 12.1 we have $\delta = -1$ and

$$f_\tau'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + 2\tau\theta^2 G(r) \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - \tfrac{1}{2}H(r, \tfrac{1}{2})/G(r)\} + o(\theta^2).$$

Now $H(r, w)$ is an increasing function of w in $0 \leqq w \leqq \frac{1}{2}$ so $H(r, \frac{1}{2}) > 2G(r)$. Also $\frac{1}{2}\tau \tan \frac{1}{2}\tau \to 0$ as $\tau \to 0$, so the term in curly brackets is negative. Thus $|f_\tau'(\frac{1}{2})| < \tau |\cos \frac{1}{2}\tau|$ for small τ as $\theta \to 0$.

If $\theta_0 = \pi/2$ then in Lemma 12.2 we have $\delta = 1$ and

$$f_\tau'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + \epsilon\tau \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - 1\} + o(\epsilon).$$

Hence $|f_\tau'(\frac{1}{2})| < \tau |\cos \frac{1}{2}\tau|$ for small τ as $\theta \to \pi/2$.

Thus for all sufficiently small positive τ the extremal function is $\sin \tau z$.

14. Completion of the proof. We know that $f(z) = (-1)^k \sin 2k\pi z$ is the extremal function in $\mathfrak{F}_\tau$ in case $\tau = 2k\pi$. However, in the intervals

$$\chi_n < \tau < \gamma_n, \qquad n = 0, 1, 2, \cdots, \tag{14.1}$$

the extremal function in $\mathfrak{F}_\tau$ is $\sin \psi(z)$, where $\psi(z)$ is defined by (10.3), (10.5). For, if τ lies in the subinterval $\chi_n < \tau \leqq (2n+1)\pi$ then $\tau |\cos \frac{1}{2}\tau|$ is a decreasing function, and

$$\mathfrak{L}(\pm \sin \tau z) = \pm 2\tau \cos \tfrac{1}{2}\tau < (-1)^n 2\chi_n \cos \tfrac{1}{2}\chi_n = \mathfrak{L}((-1)^n \sin \chi_n z).$$

Thus for $\chi_n < \tau \leqq (2n+1)\pi$ the extremal function is not $\pm \sin \tau z$ and is therefore $\sin \psi(z)$.

If τ lies in a subinterval $(2n+1)\pi < \tau < \gamma_n$ we shall define a function $f(z)$ belonging to $\mathfrak{F}_\tau$ such that $|f'(\frac{1}{2})| > \tau |\cos \frac{1}{2}\tau|$. For each θ in $0 < \theta < \pi/2$ define α and r by (11.4) with $m = 0$. Thus α and r are functions of θ for each fixed τ, and $r \to r_0 = \pi/(2\tau) < \frac{1}{2}$ as $\theta \to 0$. Substituting these values of α, r, θ with $\delta = \pm 1$ in (10.3), (10.5), we obtain a function $\psi^*(z)$, depending on τ and θ. Then $f^*(z) = \sin \psi^*(z)$ is entire and belongs to $\mathfrak{F}_\tau$. If τ is fixed and $\theta \to 0$, Lemma 12.3 shows that

$$\delta f^{*\prime}(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau - 4\theta^2 \tau r_0^2 (1 - 4r_0^2)^{-1} \times \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau + (1 + 4r_0^2)/(1 - 4r_0^2)\} + o(\theta^2).$$

Since τ lies in some interval $(2n+1)\pi < \tau < \gamma_n$ the term in curly brackets is negative. Thus if θ is small, for suitable choice of $\delta = \pm 1$, we have $f^{*\prime}(\frac{1}{2}) > \tau \mid \cos \frac{1}{2}\tau \mid$. The extremal function in $\mathfrak{F}_\tau$ therefore cannot be $\pm \sin \tau z$ and hence must be $\sin \psi(z)$ for some $\psi(z)$ defined by (10.3), (10.5).

Suppose now that for some τ_1 the extremal function is $f_{\tau_1}(z) = \sin \psi_{\tau_1}(z)$. Since $f_\tau(z)$ is a continuous function of τ there is an open interval containing τ_1 for which the extremal function is not $\pm \sin \tau z$ and therefore is $\sin \psi_\tau(z)$. Let (τ', τ'') be the largest such interval containing τ_1. Then

$$f_{\tau'}(z) = \pm \sin \tau' z, \qquad f_{\tau''}(z) = \pm \sin \tau'' z, \tag{14.2}$$

and $f_\tau(z) = \sin \psi_\tau(z)$ for $\tau' < \tau < \tau''$, where $\psi_\tau(z)$ is given by (10.3) and the parameters satisfy (10.7), (10.8) (or (11.4)). Also $\delta = \pm 1$ is such that $\mathfrak{L}(f_\tau) > 0$.

We have to prove that, for some n, $\tau' = \chi_n$, $\tau'' = \gamma_n$.

We note first that because of (14.2) the points τ', τ'' lie outside all the intervals (14.1). Also, since $f_\tau(z)$ depends continuously on τ the parameters θ, α, r are continuous functions of τ for $\tau' < \tau < \tau''$. Thus in (11.8) the integer m must be the same for all τ in $\tau' < \tau < \tau''$.

Now let τ approach one of the endpoints of (τ', τ'') from inside through a sequence of values such that $\theta = \theta(\tau)$ tends to a limit, and $r = r(\tau)$ tends to a limit, finite or infinite. We shall denote this endpoint by τ^*, and write $\theta \to \theta^*$, $0 \leqq \theta^* \leqq \pi/2$.

We show first that $\theta^* = 0$ or $\pi/2$. For, if $0 < \theta^* < \pi/2$ and $r \to \infty$ then (10.7) or (11.4) shows that α/r^2 approaches a limit A, $-1 < A < 1$. Then (10.3), (10.5) show that $f_\tau(z) \to \pm \sin \tau^* A z$, and this contradicts (14.2). If $0 < \theta^* < \pi/2$ and r tends to a finite limit r^* then (11.7) shows that α also tends to a finite limit α^*. Then $\psi_\tau(z)$ tends to a limit defined by (10.3), (10.5) for the parametric values θ^*, r^*, α^* as $\tau \to \tau^*$. This again contradicts (14.2).

If $\theta^* = 0$, then, by Lemma 11.5, the right-hand side of (10.8) approaches -1 and, since m is fixed, this shows that r cannot tend to 0 or ∞. Thus $0 < r^* < \infty$. In case $r^* > \frac{1}{2}$ Lemma 12.1 shows that

$$-\delta f'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + 2\tau\theta^2 G(r) \cos \tfrac{1}{2}\tau \{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - \tfrac{1}{2}H(r, \tfrac{1}{2})/G(r)\} + o(\theta^2).$$

Since τ lies in (τ', τ'') and $f(z)$ is an extremal function we have $|f'(\frac{1}{2})| \geqq |\cos \frac{1}{2}\tau|$. Thus the term in curly brackets is nonnegative, and so is its

limit as $\tau \to \tau^*$. Now $H(r^*, w)$ is an increasing function of w in $0 \leqq w \leqq \frac{1}{2}$, so $H(r^*, \frac{1}{2}) > 2G(r^*)$. Thus

$$\tfrac{1}{2}\tau^* \tan \tfrac{1}{2}\tau^* \geqq \tfrac{1}{2}H(r^*, \tfrac{1}{2})/G(r^*) > 1.$$

This shows that τ^* lies in some interval $(\chi_n, (2n+1)\pi] \subset (\chi_n, \gamma_n)$, but this has been excluded.

If $\theta^* = 0$, then $r^* \leqq \frac{1}{2}$, and we now show that $r^* < \frac{1}{2}$. For if $r^* = \frac{1}{2}$, then Lemma 11.5 shows that $(2m-1)\pi/\tau \to -1$ as $\tau \to \tau^*$. But τ^* cannot lie in any interval (14.1), so this is a contradiction.

If $\theta^* = 0$, we show that $\tau^* = \gamma_n$ for some n. For, we have shown that $r^* < \frac{1}{2}$, so Lemma 12.3 applies. Thus

$$\delta f'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau - 4\theta^2 \tau r^{*2}(1-4r^{*2})^{-1}$$
$$\times \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau + (1+4r^{*2})/(1-4r^{*2})\} + o(\theta^2),$$

where, by Lemma 11.5,

$$r^* = \lim r = (\tfrac{1}{2} - m)\pi/\tau^*. \tag{14.3}$$

Since τ lies in (τ', τ'') and f is an extremal function we know that $|f'(\frac{1}{2})| > \tau |\cos \frac{1}{2}\tau|$. The term in curly brackets is therefore nonpositive, and so is its limit as $\tau \to \tau^*$. Thus

$$\tfrac{1}{2}\tau^* \tan \tfrac{1}{2}\tau^* \leqq -(1+4r^{*2})/(1-4r^{*2}). \tag{14.4}$$

We recall that $0 < r^* < \frac{1}{2}$. Then in (14.3), m is 0 or a negative integer. The point τ^* cannot lie in any interval (14.1), and this shows both that (14.4) is an equality and that $m = 0$ in (14.3). Thus $\tau^* = \gamma_n$ for some n. Now m in (14.3) is the same integer m that occurs in (10.8) for all τ in the interval $\tau' < \tau < \tau''$. Thus if $\theta^* = 0$ then for all τ in $\tau' < \tau < \tau''$ the parameters of the extremal function satisfy (10.8) with $m = 0$.

If $\theta^* = \pi/2$ then Lemma 12.2 shows that

$$\delta f'(\tfrac{1}{2}) = \tau \cos \tfrac{1}{2}\tau + \epsilon\tau \cos \tfrac{1}{2}\tau\{\tfrac{1}{2}\tau \tan \tfrac{1}{2}\tau - 1\} + o(\epsilon).$$

Since f is an extremal function we have $|f'(\frac{1}{2})| > \tau |\cos \frac{1}{2}\tau|$, and since $\tau \to \tau^*$ this implies that $\frac{1}{2}\tau^* \tan \frac{1}{2}\tau^* \geqq 1$. If this were a strict inequality, τ^* would lie in one of the intervals (14.1), and this is impossible. Thus $\tau^* = \chi_n$ for some n.

We have thus shown that the open interval (τ', τ'') has its end points in the sets $\{\chi_n\}$, $\{\gamma_n\}$. On the other hand, the interval cannot contain any point $2k\pi$ since at these points the extremal function in $\pm \sin 2k\pi z$. It

follows that for some nonnegative n we have $\tau' = \chi_n$, $\tau'' = \gamma_n$. Then $\theta \to \pi/2$ as $\tau \to \tau' = \chi_n$ and $\theta \to 0$ as $\tau \to \tau'' = \gamma_n$ through values in (τ', τ'').

As τ moves from τ' to τ'' the angle θ moves from $\pi/2$ to 0, taking all values in $(0, \pi/2)$. The parameters satisfy (10.7), (10.8), or (11.3), (11.4), with $m = 0$. The left-hand side of (10.8) is never zero for $\tau' < \tau < \tau''$, so the right-hand side of (10.8) is never zero for $0 < \theta < \pi/2$ when the value of α/r^2 in (10.8) is that determined by (10.7).

In the intervals in which the extremal function has the form $\sin \psi(z)$, the maximum of $\mathcal{L}(f)$ could be calculated for any given τ by determining α and r from (11.3), (11.4) and calculating the maximum of $\mathcal{L}(f)$ as a function of θ.

15. Functionals which involve no derivatives. If all $n_\nu = 0$ in (2.1), i. e., if $\mathcal{L}(f)$ has the form

$$\mathcal{L}(f) = \sum_{\nu=1}^{m} \alpha_\nu f(x_\nu), \tag{15.1}$$

Theorem 1 does not apply. For example, if

$$\mathcal{L}(f) = f(\tfrac{1}{2}) - f(-\tfrac{1}{2}), \tag{15.2}$$

then when $\tau > \pi$, an obvious extremal function is $f(z) = \sin \pi z$, which is of type less than τ; and if $\tau > 3\pi$ another extremal function is $f(z) = -\sin \frac{3}{2}\pi z$, so that the extremal function is not unique. However, functionals (15.1) can be discussed by using the following device. Consider the functional

$$\mathcal{L}_t(f) = tf'(x_1) + \mathcal{L}(f), \qquad t > 0. \tag{15.3}$$

This is a functional of order $m + 1$ to which our theory applies for each t. Let $f_t(z)$ be the extremal function for $\mathcal{L}_t$. Then $\{f_t(z)\}$, where t runs through a sequence whose limit is 0, is a normal family; let $f_0(z)$ be a limit function of this family. Then f_0 is an extremal function for the functional $\mathcal{L}$. For, by Bernstein's theorem,

$$\mathcal{L}(f_t) = \mathcal{L}_t(f_t) - tf_t'(x_1) \geqq \mathcal{L}_t(f_t) - t\tau.$$

We know from Lemma 2.2 that there is at least one extremal function f_1 for $\mathcal{L}$. Then

$$tf_t'(x_1) + \mathcal{L}(f_t) = \mathcal{L}_t(f_t) \geqq \mathcal{L}_t(f_1) = tf_1'(x_1) + \mathcal{L}(f_1).$$

Since $f_t'(x_1) \to f_0'(x_1)$ and $\mathcal{L}(f_t) \to \mathcal{L}(f_0)$, it follows that $\mathcal{L}(f_0) \geqq \mathcal{L}(f_1)$.

Since f_1 is extremal for $\mathcal{L}$, so is f_0, and $\mathcal{L}(f_0)=\mathcal{L}(f_1)$. Now since f_t is of order $m+1$, either f_t is a constant or

$$f_t(z)=\sin\psi_t(z), \tag{15.4}$$

where

$$\psi_t(z)=\pm\tau\int_0^z\{q_t(w)\}^{-\frac{1}{2}}p_t(w)\,dw+\sin^{-1}f_t(0), \tag{15.5}$$

p_t is of degree at most $m-1$ and q_t is of degree twice that of p_t, and the other conclusions of Theorem 1 hold.

As $t\to 0$ either the coefficients of p_t and q_t are bounded and we can select a sequence of t's so that p_t and q_t approach limits of the same kind; or the coefficients of p_t and q_t are unbounded, in which case the integrand of $\psi_t(z)$ approaches a function of the same form, $p(w)/\{q(w)\}^{\frac{1}{2}}$, but with p and q not necessarily monic. Hence we can obtain an extremal function for $\mathcal{L}$ by taking either a constant, or a function of the form described in Theorem 1, or one of the same form with p of degree at most $l-2$, but with τ possibly replaced by a smaller number.

The simplest nontrivial functional of the kind under consideration is $\mathcal{L}(f)=f(\frac{1}{2})-f(-\frac{1}{2})$, which was considered by S. Bernstein [1]. He showed that an extremal function is $\sin\tau z$ if $0<\tau\leqq\pi$, when $\max\mathcal{L}(f)=2\sin\frac{1}{2}\tau$ (see also [2], p. 214); while if $\tau>\pi$ an extremal function is $\sin\pi z$ and $\max\mathcal{L}(f)=2$. Here, although the variational method can be used, it is not advantageous since the extremal functions can be completely determined by more direct methods. The same is true for

$$\mathcal{L}(f)=f(-1)-2f(0)+f(1).$$

However, the less symmetrical functional

$$\mathcal{L}(f)=f(-1)+f(0)-f(1)$$

is better suited to our method. For possible extremal functions of the form $\sin(\sigma z+c)$ we have $\max\mathcal{L}(f)=(1+4\sin^2\sigma)^{\frac{1}{2}}$, which is actually extremal for sufficiently small σ. On the other hand, our method also suggests possible extremal functions of the form

$$f(z)=\pm\cos\sigma\sqrt{(z^2+2rz\cos\phi+r^2)}, \tag{15.6}$$

and for sufficiently large σ we can make $\mathcal{L}(f)$ for such a function attain the largest possible value, namely 3. Hence there is a number σ such that (15.6) is an extremal function for $\mathcal{L}$ in $\mathfrak{F}_\tau$ for all $\tau\geqq\sigma$. It is possible

that functions of the kind considered in Theorem 5 are extremal for an intermediate range of values of τ, but we have not investigated this possibility.

NORTHWESTERN UNIVERSITY,
UNIVERSITY OF WISCONSIN.

REFERENCES.

[1] S. Bernstein, "Extension of an inequality of S. B. Stechkin to entire functions of finite degree," *Doklady Akademiya Nauk SSSR*, vol. 60 (1948), pp. 1487-1490 = Sobranie Sochinanii, vol. 2, 1954, Akademiya Nauk SSSR, pp. 442-445.

[2] R. P. Boas, Jr., *Entire functions*, Academic Press, New York, 1954.

[3] ———, and A. C. Schaeffer, "New inequalities for entire functions," to appear in *Journal of Mathematics and Mechanics*.

[4] P. L. Chebyshev, "Théorie des mécanismes connus sous le nom de parallélogrammes," *Mémoires de l'Académie de Sciences de St. Pétersbourg*, vol. 7 (1854), pp. 539-568 = Polnoe Sobranie Sochinenii, vol. 2, Moscow-Leningrad, 1947, pp. 23-51.

[5] F. Oberhettinger and W. Magnus, *Anwendung der elliptischen Funktionen in Physik und Technik*, Springer, Berlin-Göttingen-Heidelberg, 1949.

[6] G. Zolotareff, "Sur l'application des fonctions elliptiques aux questions de maxima et minima," *Bulletin de l'Académie des Sciences de St.-Pétersbourg* (3), vol. 24 (1878), pp. 305-310; *Oeuvres*, vol. 1, pp. 369-374; vol. 2, pp. 130-166.

ON KAEHLERIAN HOMOGENEOUS SPACES OF UNIMODULAR LIE GROUPS.*

By JUN-ICHI HANO.

Recently the results of E. Cartan on Hermitian symmetric space have been extended to the case of Kaehlerian homogeneous spaces by several authors. In particular the structure of compact Kaehlerian homogeneous spaces has been fully exploited. As for the non-compact case, there are few known results except in the case where the groups are semi-simple or reductive. A. Borel [1] and J. L. Koszul [6] have studied the structure of Kaehlerian homogeneous spaces of semi-simple Lie groups and have shown, independently of each other, an interesting result that a bounded domain in a unitary space admitting a transitive semi-simple Lie group of complex analytic homeomorphisms is symmetric. This result gives a partial answer to the problem of E. Cartan. In his important paper in 1935 [2], E. Cartan raised the question whether a bounded homogeneous domain is always a symmetric bounded domain. Y. Matsushima [8] has studied the structure of Kaehlerian homogeneous spaces of reductive Lie groups and has shown that these spaces are the direct product of a locally flat Kaehlerian space and a Kaehlerian homogeneous space of a semi-simple Lie group.

The purpose of the present paper is to study the structure of Kaehlerian homogeneous spaces of a more general class of Lie groups, that is, those of unimodular Lie groups. Specifically, we shall deal with the following two cases. First we shall consider the case where the isotropy group is semi-simple and obtain the following two theorems:

THEOREM I. *If a homogeneous space of a connected unimodular Lie group by a closed connected semi-simple subgroup admits an invariant Kaehlerian structure, then the Kaehlerian structure is locally flat.*

THEOREM II. *If a connected unimodular Lie group has a left invariant Kaehlerian structure, then the group is meta-abelian. Especially if the group is nilpotent, then it must be abelian.*[1]

* Received April 15, 1957; revised September 18, 1957.

[1] The last part of Theorem 2 is a generalization of a result of Koszul (unpub-

Secondly we deal with a Kaehlerian homogeneous space of a unimodular Lie group whose Ricci curvature is non-degenerate and prove the following:

THEOREM III. *If the Ricci curvature of a Kaehlerian homogeneous space of a connected unimodular Lie group is non-degenerate and if the group acts effectively on the space, then the group is semi-simple.*

A bounded domain in a unitary space has the Bergman metric which is Kaehlerian and invariant by all complex analytic homeomorphisms of the domain. If a bounded domain admits a transitive group of complex analytic homeomorphisms, the Ricci curvature of the Bergman metric coincides with the metric itself, and hence it is positive definite. Therefore, from Theorem III and from the result of A. Borel and J. L. Koszul mentioned above, we have the following answer to the problem of E. Cartan:

THEOREM IV. *A bounded domain which admits a transitive connected unimodular Lie group of complex analytic homeomorphisms is symmetric.*

We remark that these theorems hold true under a slightly weaker assumption which is explained in **4**, and that in order to prove Theorem III, we only use the result in **6** concerning the Ricci curvature of a Kaehlerian homogeneous space.

The author wishes to express here his sincere thanks to Professor Y. Matsushima and Professor K. Nomizu for their kind suggestions and valuable criticism during the preparation of this paper.

I. Preliminaries.

1. Let G be a connected Lie group and let B be a closed subgroup of G. We denote by $\mathfrak{g}$ the Lie algebra of all left invariant vector fields on G and by $\mathfrak{b}$ the subalgebra of $\mathfrak{g}$ consisting of all left invariant vector fields which are tangent to B at the identity e. Let G/B be the homogeneous space of left cosets of G by B, and let π be the projection from G onto G/B. The differential π_e of π at the identity e maps the tangent space $\mathfrak{g}_e$ of G at e onto the tangent space T_o of G/B at o, where o denote the point $\pi(e)$. By assigning $\pi_e(X_e)$ to each $X \in \mathfrak{g}$, we have the linear mapping π' from $\mathfrak{g}$ onto T_o, where X_e is the value at e of the vector field X.

When $\mathfrak{g}$ has a direct sum decomposition $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ into two subspaces

lished). He has proved the same result for rational nilpotent Lie groups. He has also proved that if a compact homogeneous space of a nilpotent Lie group admits a Kaehlerian structure, not necessarily invariant, the group must be abelian.

$\mathfrak{b}$ and $\mathfrak{m}$ such that $\mathrm{ad}\, b \cdot \mathfrak{m} \subset \mathfrak{m}$ for all $b \in B$, the homogeneous space G/B is called a reductive homogenous space by Nomizu [10]. We shall call this decomposition of $\mathfrak{g}$ an $\mathrm{ad}\, B$-stable decomposition. When, more strongly, the induced representation of B on the Grassmann algebra of $\mathfrak{g}$ is completely reducible, we say that the subgroup B is reductive in G according to Koszul [5]. Clearly, if B is reductive in G, G/B is a reductive homogeneous space.

A homogeneous space G/B having a Riemannian metric invariant by the group G is called a Riemannian homogeneous space. We shall prepare the following proposition for later use.

(1.1) *Let G/B be a Riemannian homogeneous space. If G operates effectively on G/B, then the subgroup B is reductive in G.*

In fact, let us consider the largest connected group G^* of isometries. It is known that G^* is a Lie group and the isotropy subgroup B^* at o is compact. Hence the Lie algebra $\mathfrak{g}^*$ of G^* has a positive definite symmetric bilinear form f^* invariant by $\mathrm{ad}\, b$ for all $b \in B^*$. Since G is effective on G/B, G can be embedded in G^* as a Lie subgroup. The restriction f of f^* on the subalgebra $\mathfrak{g}$ is evidently a positive definite symmetric bilinear form and invariant by $\mathrm{ad}\, b$ for all $b \in B$. The Grassmann algebra of $\mathfrak{g}$ has a positive definite symmetric bilinear form induced by f, which is invariant by the induced representation of B on the Grassmann algebra. Therefore this representation is completely reducible, and our assertion is proved.

2. Let G/B be a reductive homogeneous space and let $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ be an $\mathrm{ad}\, B$-table decomposition. The subscript $\mathfrak{m}$ (resp. $\mathfrak{b}$) of an element X in $\mathfrak{g}$ means the $\mathfrak{m}$-component (resp. the $\mathfrak{b}$-component) of X with respect to this decomposition. The restriction of π' on $\mathfrak{m}$ gives an isomorphism from $\mathfrak{m}$ onto T. Hereafter, when we consider a reductive homogeneous space, we shall identify the tangent space T_o of G/B at o with the subspace $\mathfrak{m}$ by this isomorphism.

Now, we assume that G/B has an invariant Riemannian metric g. Following Nomizu [9], we shall prepare some fundamental notions of an invariant Riemannian connection on G/B. Let X be an element in $\mathfrak{m}$. We denote by σ_t the one-parameter subgroup generated by $X \in \mathfrak{m}$. We set $\sigma_t \cdot o = \tau_t$. Clearly σ_t defines the type preserving isomorphism from the tensor algebra at o onto the tensor algebra at τ_t, which we denote also by σ_t. Moreover, we denote by ρ_t^{-1} the parallel translation from τ_t to o along the curve τ_t in the opposite direction, which is defined by the Riemannian connection associated to the metric g. We have the linear mapping D_X of the tensor algebra of $\mathfrak{m}$ defined by

$$D_X A = \lim_{t\to 0}(\rho_t^{-1}\cdot \sigma_t A - A)/t, \text{ where } t\to 0,$$

for all tensors A on $\mathfrak{m}$. Clearly D_X preserves the type of tensors and is linear with respect to X. Moreover, D_X satisfies the following conditions:

(2.1) $\operatorname{ad} b\cdot D_X Y = D_{\operatorname{ad} b\cdot X}\operatorname{ad} b\cdot Y$ for all $X, Y\in\mathfrak{m}$ and for all $b\in B$.

(2.2) $g(D_X Y, Z) + g(Y, D_X Z) = 0$ for all $X, Y, Z\in\mathfrak{m}$.

(2.3) $D_X Y - D_Y X - [X, Y]_{\mathfrak{m}} = 0$ for all $X, Y\in\mathfrak{m}$.

(2.4) If a tensor field a on G/B is G-invariant, $D_X a$ coincides with the covariant derivative of a at $\circ$ along X.

The value at $\circ$ of the curvature tensor field R, of type (1.3), is given by

$$R_\circ(X, Y)Z = [D_X, D_Y]Z - D_{[X,Y]_{\mathfrak{m}}}Z - \operatorname{ad}[X, Y]_{\mathfrak{b}}Z$$

for all $X, Y, Z\in\mathfrak{m}$. The value at $\circ$ of the Ricci curvature r is given by $r_\circ(X, Y) = \operatorname{tr}_{\mathfrak{m}}(Z\to R_\circ(Y, Z)X)$ for all $X, Y\in\mathfrak{m}$.

Let G/B be a simply connected Riemannian homogeneous space. Since a Riemannian homogeneous space is complete, G/B has the canonical decomposition with respect to the homogeneous holonomy group given by de Rahm [3]. G/B is a Riemannian direct product of spaces $M_\circ, M_1,\cdots, M_s$, where $M_\circ$ is a Euclidean space and M_i, $1\leqq i\leqq s$, has the non-trivial irreducible homogeneous holonomy group. Moreover each M_i is isometric to the Riemannian homogeneous space G_i/B of a connected closed subgroup G_i in G containing the subgroup B ([10], Theorem 3). We can denote this decomposition by $G_\circ/B\times G_1/B\times\cdots\times G_s/B$.

Now let I be a G-invariant tensor field of type (1,1) defining an invariant complex structure on a homogeneous space G/B. By a result of Koszul [6], the value $I_\circ$ at $\circ$ of I satisfies the following conditions:

$$(\operatorname{ad} b)_{\mathfrak{m}}\cdot I_\circ = I_\circ\cdot(\operatorname{ad} b)_{\mathfrak{m}} \text{ for all } b\in \mathrm{B},$$

$$I_\circ[X, Y]_{\mathfrak{m}} - [I_\circ X, Y]_{\mathfrak{m}} - [X, I_\circ Y]_{\mathfrak{m}} - I_\circ[I_\circ X, I_\circ Y]_{\mathfrak{m}} = 0 \quad \text{for all } X, Y\in\mathfrak{m}.$$

When G/B has an invariant complex structure, an invariant Riemannian metric g on G/B is called Hermitian if g satisfies the condition: $g(IX, IY) = g(X, Y)$ for any vector fields X, Y on G/B. In this case we have a 2-form Ω given by $\Omega(X, Y) = g(IX, Y)$ for all vector field X, Y on G/B, which is called the Kaehlerian form associated to the Hermitian metric g. Of course, Ω is G-invariant. If the Kaehlerian form Ω is a cocycle, that is,

$d\Omega = 0$ we call the pair of the complex structure I and the Hermitian metric g an invariant Kaehlerian structure. A homogeneous space having an invariant Kaehlerian structure is called a Kaehlerian homogeneous space. It is well known that a G-invariant Hermitian metric g on a complex homogeneous space G/B, defines a Kaehlerian structure if and only if the covariant differential of the tensor field I is equal to zero. When G/B is a reductive homogeneous space, this condition is equivalent to the following:

$$D_X \cdot I_\circ = I_\circ \cdot D_X \quad \text{for all } X \in \mathfrak{m}. \tag{2.5}$$

The value at $\circ$ of the Ricci curvature r associated to an invariant Kaehlerian structure may be expressed by

$$r_\circ(X, Y) = \tfrac{1}{2}\mathrm{tr}_{\mathfrak{m}} I_\circ \cdot R(I_\circ X, Y),$$

a formula which is equivalent to the one in [7]. The bilinear form defined by $\alpha(X, Y) = r(IX, Y)$ for all vector fields X, Y is a G-invariant exterior form of degree two. We call this 2-form α the Ricci form.

3. Let $C^*(G)$ be the Grassmann algebra of all left invariant differential forms on a connected Lie group G. Let $C^p(G)$ be the subspace of $C^*(G)$ consisting of all homogeneous elements of degree p. We denote by w the linear mapping of $C^*(G)$ such that $wa = (-1)^p a$ for all $a \in C^p(G)$. For each $a \in C^*(G)$, we have the linear mapping $\epsilon(a)$ of $C^*(G)$ given by $\epsilon(a)b = a \wedge b$ for all $b \in C^*(G)$. For each $X \in \mathfrak{g}$, we have the linear mapping $\iota(X)$ of $C^*(G)$ such that 1) $\iota(X)a = 0$ for all $a \in C^\circ(G)$ 2) if $a \in C^p(G)$ $(p \geqq 1)$,

$$(\iota(X)a)(X_1, \cdots, X_{p-1}) = \frac{1}{p}\, a(X, X_1, \cdots, X_{p-1})$$

for all $X_1, \cdots, X_{p-1} \in \mathfrak{g}$. We know that $\iota(X)$ is an anti-derivation of $C^*(G)$, i.e. $\iota(X)(a \wedge b) = \iota(X)a \wedge b + wa \wedge \iota(X)b$ for all $a, b \in C^*(G)$. Moreover, for each $X \in \mathfrak{g}$, the derivation $\theta(X)$ of $C^*(G)$ is defined by

$$(\theta(X)a)(X_1, \cdots, X_p) = -\sum_{1 \leqq i \leqq p} a(X_1, \cdots, [XX_i], \cdots, X_p)$$

for all $a \in C^p(G)$ and for all $X_1, \cdots, X_p \in \mathfrak{g}$; $\theta(X)$ is nothing but an infinitesimal transformation defined by the right invariant vector field X' whose value at e coincides with X_e. If $a \in C^*(G)$, the exterior differential da is also contained in $C^*(G)$. The following relation among these operations will be used frequently:

$$\theta(X) = \iota(X)d + d\iota(X). \tag{3.1}$$

We denote by $H^*(G)$ the cohomology algebra of $C^*(G)$ with respect to the coboundary operator d.

Let G/B be a homogeneous space of a connected Lie group G. We denote by $C^*(G/B)$ the space of all G-invariant differential forms on G/B. Clearly $C^*(G/B)$ is finite dimensional over the field of all real numbers. We denote $C^p(G/B)$ the subspace of all homogeneous elements of degree p. Since the exterior differential da of $a \in C^*(G/B)$ also belongs to $C^*(G/B)$, we have the cohomology algebra $H^*(G/B)$ of $C^*(G/B)$ with respect to d. Let π^* be the dual of the differential of the projection π from G onto G/B, and let $L^*(G/B)$ be the image of $C^*(G/B)$ by π^*. Obviously $L^*(G/B)$ is a subalgebra of $C^*(G)$ and is equal to the subspace of all element $a \in C^*(G)$ such that 1) $\iota(X)a = 0$ for all $X \in \mathfrak{b}$ and 2) the right translation defined by any $b \in B$ leaves a variant. Since the exterior differentiation and π^* are commutative, $L^*(G/B)$ is d-stable.

We denote by $N^1(G:B)$ the subspace of $C^1(G)$ consisting of all elements a such that $\iota(X)a = 0$ for all $X \in \mathfrak{b}$, and by $N^*(G:B)$ the subalgebra in $C^*(G)$ generated by 1 and $N^1(G:\mathrm{B})$. The subalgebra $N^*(G:B)$ is the direct sum of its homogeneous parts $N^p(G:B) = N^*(G:B) \cap C^p(G)$, and is $\mathfrak{b}$-stable, i.e. $\theta(X)$ leaves $N^*(G:B)$ stable for all $X \in \mathfrak{b}$. We say that an element $a \in C^*(G)$ is $\mathfrak{b}$-invariant if $\theta(X)a = 0$ for all $X \in \mathfrak{b}$. We denote by $L^*(G:B)$ the subalgebra of all $\mathfrak{b}$-invariant elements in $N^*(G:B)$; $L^*(G:B)$ is the direct sum of its homogeneous parts $L^p(G:B) = L^*(G:B) \cap C^p(G)$. In virtue of (3.1), the exterior differentiation d leaves $L^*(G:B)$ stable. We can easily see that the subalgebra $L^*(G/B)$ is contained in $L^*(G:B)$ and that if B is connected, $L^*(G:B)$ coincides with $L^*(G/B)$.

For an arbitrary differential form a on a manifold, we have also the operation $\epsilon(a)$ which maps any differential form b to $a \wedge b$. When a manifold has a Riemannian metric g, we have the dual operation $\iota(a)$ of $\epsilon(a)$ given by $g(\iota(a)b, c) = g(b, \epsilon(a)c)$ for all differentials forms b and c.

4. Later on we shall have frequently to do with the condition that the highest dimensional homogeneous part of $H^*(G/B)$ does not vanish, which we now explain. This condition is equivalent to the following two conditions: 1) there exists a G-invariant n-form, where $n = \dim G/B$, and 2) $dC^{n-1}(G/B) = 0$. By a theorem given by Koszul ([5], Theorem 12.1), we know that if a connected Lie group G is unimodular and if a closed connected subgroup B is reductive in G, then $\dim H^n(G/B) = 1$. We prove the following proposition:

(4.1) *If a Riemannian homogeneous space of a connected unimodular Lie group G is orientable and if G acts effectively on G/B, then* $\dim H^n(G/B) = 1$.

In fact, since G/B is orientable, there exists a G-invariant non-zero n-form, the so-called volume element. Since G is effective on G/B, we have, as is already seen in **1**, a positive definite symmetric bilinear form on the Lie algebra $\mathfrak{g}$, which is $\operatorname{ad} b$-invariant for all $b \in B$. Hence, the connected component $B_\circ$ of B is also reductive in G. Applying the above theorem of Koszul for the pair of G and $B_\circ$, we have $dC^{n-1}(G/B_\circ) = 0$ and hence $dL^{n-1}(G/B_\circ) = 0$. Since $B_\circ$ is connected, we have $dL^{n-1}(G:B_\circ) = 0$. Clearly $L^{n-1}(G/B)$ is contained in $L^{n-1}(G:B_\circ)$, and hence we have $dL^{n-1}(G/B) = 0$, which implies $dC^{n-1}(G/B) = 0$. Thus our assertion is proved.

Conversely, if $\dim H^n(G/B) = 1$, the space G/B is orientable.

II. Invariant forms on a Riemannian homogeneous space.

5. Let us consider an orientable n-dimensional Riemannian homogeneous space G/B with metric tensor field g. Since G/B is orientable, there exists a differential form v of degree n which is invariant by G and has the unit length. Making use of v, the star operator $*$ is defined by $*a = \iota(a)v$ for any differential form a on G/B. We define the codifferential operator δ by $\bar{w} * d * w$, where w (resp. $\bar{w}$) is the linear mapping such that $wa = (-1))^p a$ (resp. $\bar{w}a = (-1)^{p(n+1)}a$) for any p-form a. The Laplacian operator Δ is given by $\delta d + d\delta$, and we say that a differential form a is harmonic if and only if $\Delta a = 0$. Since these operators commute with the transformations in G, they leave $C^*(G/B)$ stable.

We shall give expressions of the operators d, δ and Δ in terms of covariant differentiation. For this purpose, let us take a frame $\{X_1, \cdots, X_n\}$ on an open set and let $\{\omega^1, \cdots, \omega^n\}$ be the dual frame of $\{X_1, \cdots, X_n\}$. Then we have

$$d = \sum_{1 \leqq i \leqq n} \epsilon(\omega^i) \nabla_{X_i}, \qquad \delta = -\sum_{1 \leqq i \leqq n} \iota(\omega^i) \nabla_{X_i},$$

where ∇_X denotes the covariant differentiation along the vector field X. If a is a 1-form, we have

$$\Delta a = -\sum_{1 \leqq i \leqq n} (\nabla_{X_i} \nabla_{X_i} - \nabla_{\nabla_{X_i} X_i}) a - \sum_{1 \leqq i, j \leqq n} \epsilon(\omega^i) \iota(\omega^j) R(X_i, X_j) a.$$

When a is a G-invariant 1-form, $g(a, a)$ is a constant over GB, and hence we have $g(\nabla_X a, a) = 0$. It follows that if $a \in C^1(G/B)$, then

$$g(\Delta a, a) = \sum_{1\leqq i\leqq n} g(\nabla_{X_i} a, \nabla_{X_i} a) - r(a, a),$$

where r is the bilinear form on $C^1(G/B)$ given by the Ricci curvature r. On account of this formula, we obtain the following proposition:

(5.1) *Let G/B be an orientable Riemannian homogeneous space. If a G-invariant 1-form a on G/B is harmonic and if $r(a,a)=0$, then a is a parallel field.*

Now, we restrict our consideration to $C^*(G/B)$. For any two elements $a, b \in C^*(G/B)$, $g(a,b)$ is a constant over G/B. We can regard g as an inner product on the finite dimensional vector space $C^*(G/B)$ over the field of all real numbers. Using a property of the star operator, we have

$$*d(a_\wedge * b) = *(da_\wedge * b) + *(wa_\wedge d*b) = g(da, b) - g(a, \delta b)$$

for all $a \in C^p(G/B)$, $b \in C^{p+1}(G/B)$, $0 \leqq p \leqq n$. Let us assume that $\dim H^n(G/B) = 1$. Then the exterior differential of any G-invariant $(n-1)$-form is zero and we have $g(da, b) = g(a, \delta b)$ for all $a \in C^p(G/B)$, $b \in C^{p+1}(G/B)$. If $b \in C^q(G/B)$, $q \neq p+1$, it is clear that $g(da, b) = g(a, \delta b) = 0$. Therefore we have $g(da, b) = g(a, \delta b)$ for all $a, b \in C^*(G/B)$. Moreover, we have $g(\Delta a, a) = g(da, da) + g(\delta a, \delta a)$. This equality shows that a G-invariant differential form a is harmonic if and only if $da = \delta a = 0$, in other words, if and only if a is orthogonal to the subspaces $dC^*(G/B)$ and $\delta C^*(G/B)$. On the other hand, the subspaces $dC^*(G/B)$ and $\delta C^*(G/B)$ are mutually orthogonal to each other. As is already mentioned, $C^*(G/B)$ is finite dimensional. Hence we obtain the proposition:

(5.2) *Let G/B be an n-dimensional Riemannian homogeneous space of a connected Lie group. If $H^n(G/B) \neq \{0\}$, any G-invariant form a on G/B has the unique decomposition $a = a_0 + a_1 + a_2$ such that a_0 is a G-invariant harmonic form, $a_1 \in dC^*(G/B)$ and $a_2 \in C^*(G/B)$.*

III. The Ricci curvature.

6. Let G/B be a reductive homogeneous space admitting a G-invariant Kaehlerian structure which is defined by the pair of an invariant complex structure I and an invariant Hermitian metric g. We take an $\operatorname{ad} B$-stable decomposition $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$. The Ricci curvature r is equal to the canonical hermitian form defined by Koszul [6]. Hence the image $\pi^*\alpha$ of the Ricci form α is an exterior differential of a left invariant 1-form on G by a theorem of Koszul ([6], Theorem 1). We shall give a different approach to this fact from the view-point of differential geometry.

Let us consider the 1-form η in $C^*(G)$ given by

$$\eta(X) = -\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (\operatorname{ad} X_{\mathfrak{b}})_{\mathfrak{m}} \text{ for all } X \in g.$$

Since $I_\circ$ commutes with the restriction $(\operatorname{ad} b)_{\mathfrak{m}}$ of $\operatorname{ad} b$ on $\mathfrak{m}$ for all $b \in B$, we have

$$\begin{aligned}(\operatorname{ad} b\eta)(X) &= -\operatorname{tr}_{\mathfrak{m}} I_\circ . (\operatorname{ad}(\operatorname{ad} b \cdot X)_{\mathfrak{b}})_{\mathfrak{m}} \\ &= -\operatorname{tr}_{\mathfrak{m}} (\operatorname{ad} b)_{\mathfrak{m}}, \cdot I_\circ \cdot (\operatorname{ad} X_{\mathfrak{b}}) \cdot (\operatorname{ad} b)_{\mathfrak{m}}^{-1} = \eta(X),\end{aligned}$$

which implies that η is invariant by the right translation defined by any element in B. Since $\iota(X) d\eta + d\iota(X)\eta = \theta(X)\eta = 0$ for all $X \in \mathfrak{b}$ and since $d\iota(X)\eta = 0$ for all $X \in \mathfrak{b}$, we have $\iota(X) d\eta = 0$ for all $X \in \mathfrak{b}$. It follows that $d\eta \in N^*(G:B)$. Moreover $d\eta$ belongs to $L^*(G/B)$, because $\operatorname{ad} b \cdot d\eta = d \operatorname{ad} b \cdot \eta = 0$ for all $b \in B$. Next, let us consider the 1-form ξ in $N^*(G:B)$ defined by

$$\xi(X) = -\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot D_{X_{\mathfrak{m}}} \quad \text{for all } X \in \mathfrak{g}.$$

Using (2.1) and the fact that $(\operatorname{ad} b)_{\mathfrak{m}}$, $b \in B$, commutes with $I_\circ$, we have

$$\begin{aligned}(\operatorname{ad} b\xi)(X) &= -\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot D_{\operatorname{ad} \cdot b X_{\mathfrak{m}}} \\ &= -\operatorname{tr}_{\mathfrak{m}} (\operatorname{ad} b)_{\mathfrak{m}} \cdot I_\circ \cdot D_{X_{\mathfrak{m}}} \cdot (\operatorname{ad} b)_{\mathfrak{m}}^{-1} = \xi(X),\end{aligned}$$

which shows that ξ belongs to $L^1(G/B)$. Set $\phi = \eta + \xi$, then $d\phi \in L^2(G/B)$. By definition of the curvature tensor field R, we have

$$\begin{aligned}d\phi(X,Y) &= -\tfrac{1}{2}\phi([X,Y]) = \tfrac{1}{2}\operatorname{tr}_{\mathfrak{m}} I_\circ (\operatorname{ad}[XY]_{\mathfrak{b}})_{\mathfrak{m}} + \tfrac{1}{2}\operatorname{tr}_{\mathfrak{m}} I_\circ D_{[X,Y]_{\mathfrak{m}}} \\ &= \tfrac{1}{2}\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (R(X,Y) - [D_X, D_Y])\end{aligned}$$

for all $X, Y \in \mathfrak{m}$. According to (2.5), we have

$$\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot [D_X, D_Y] = \operatorname{tr}_{\mathfrak{m}}[I_\circ \cdot D_X, D_Y] = 0.$$

Therefore we have $d\phi(X,Y) = \pi^*\alpha(X,Y)$ for all $X, Y \in \mathfrak{m}$. Since both $d\phi$ and $\pi^*\alpha$ are contained in $L^*(G/B)$, we have $d\phi = \pi^*\alpha$. Moreover, ξ being in $L^*(G/B)$, $\pi^*\alpha$ and $d\eta$ are cohomologous in $L^*(G/B)$. Thereby we have obtained the following proposition.

(6.1) *Let G/B be a reductive Kaehlerian homogeneous space of a connected Lie group G, and let $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ be an $\operatorname{ad} B$-stable decomposition. The Ricci form α on G/B is cohomologous to the G-invariant 2-form ψ defined by* [2]

---

[2] Reading this manuscript, Koszul remarks that if a complex homogeneous space is reductive, the same result for the canonical Hermitian form is verified from his formula ([6], Theorem 1).

$$\psi_\circ(X,Y) = \mathrm{tr}_{\mathfrak{m}} I_\circ \cdot (\mathrm{ad}[X,Y]_{\mathfrak{b}})_{\mathfrak{m}} \textit{ for all } X, Y \in \mathfrak{m}.$$

We shall give a proof of the following fact:

(6.2) *The Ricci form α on a Kaehlerian homogeneous space is harmonic* [7].

Since the fact that the Ricci form is harmonic does not depend upon the Lie group acting transitively on the space, we can assume the homogeneous G/B to be reductive on account of (1,1). Therefore, applying the fact that $\pi^*\alpha = d\phi$, we have $d\alpha = 0$.

Let $\{X_1, \cdots, X_m, IX_1, \cdots, IX_m\}$ be an orthogonal frame defined on an arbitrary open set. We set $Z_\alpha = X_\alpha + (-1)^{\frac{1}{2}} IX_\alpha$, $Z_{\alpha^*} = X_\alpha - (-1)^{\frac{1}{2}} IX_\alpha$, $1 \leqq \alpha \leqq m$. Since $\alpha(IX, IY) = \alpha(X, Y)$ for all vector fields X, Y, we have $\alpha(Z_\alpha, Z_\beta) = \alpha(Z_{\alpha^*}, Z_{\beta^*}) = 0$, $1 \leqq \alpha, \beta \leqq m$. Moreover, $\sum_{1 \leqq \alpha \leqq m} \alpha(Z_\alpha, Z_{\alpha^*})$ is a constant over the open set, because the scalar $\sum_{1 \leqq \alpha \leqq m} \alpha(Z_\alpha, Z_{\alpha^*})$ is invariant by G. From the fact that $d\alpha = 0$, we have

$$\begin{aligned} 0 &= (d\alpha)(Z_\beta, Z_\alpha, Z_{\alpha^*}) \\ &= \tfrac{1}{3}((\nabla_{Z_\beta}\alpha)(Z_\alpha, Z_{\alpha^*}) + (\nabla_{Z_\alpha}\alpha)(Z_{\alpha^*}, Z_\beta) + (\nabla_{Z_{\alpha^*}}\alpha)(Z_\beta, Z_\alpha)). \end{aligned}$$

It follows that $(\nabla_{Z_\alpha}\alpha)(Z_{\alpha^*}, Z_\beta) = -(\nabla_{Z_\beta}\alpha)(Z_\alpha, Z_{\alpha^*})$, $1 \leqq \alpha, \beta \leqq m$. Using this, we have

$$\begin{aligned} (\delta\alpha)(Z_\beta) &= -\tfrac{1}{2} \sum_{1 \leqq \alpha \leqq m} ((\nabla_{Z_\alpha}\alpha)(Z_{\alpha^*}, Z_\beta) + (\nabla_{Z_{\alpha^*}}\alpha)(Z_\alpha, Z_\beta)) \\ &= -\tfrac{1}{2} \sum_{1 \leqq \alpha \leqq m} (\nabla_{Z_\beta}\alpha)(Z_\alpha, Z_{\alpha^*}) = 0, \qquad 1 \leqq \beta \leqq m. \end{aligned}$$

By the same argument, we have $(\delta\alpha)(Z_{\beta^*}) = 0$, $1 \leqq \beta \leqq m$. Thus we have $\delta\alpha = 0$ and $\Delta\alpha = (d\delta + \delta d)\alpha = 0$, completing the proof.

IV. Theorems.

7. When a homogeneous space G/B has a G-invariant and non-degenerate 2-cocycle Ω, we say an invariant symplectic structure is defined on G/B. If G/B admits an invariant Kaehlerian structure, the Kaehlerian form Ω defines an invariant symplectic structure. When G/B has an invariant symplectic structure defined by a 2-cocycle Ω, the dimension of G/B is an even integer $2m$ and Ω^m, the Grassmann m-th power of Ω, is not zero. In general, an exterior form Ω of degree 2 on a real $2m$-dimensional vector space is non-degenerate if and only if $\Omega^m \neq 0$.

The purpose of this section is to prove the following:

LEMMA 1. *Let G be a connected Lie group and let B be a closed connected semi-simple subgroup of G. If the homogeneous space G/B admits an invariant symplectic structure and if $H^{2m}(G/B)=0$, where $2m=\dim G/B$, then B is a maximal connected semi-simple subgroup of G.*[3]

Let Ω be a G-invariant 2-cocycle on G/B defining the invariant symplectic structure. We denote by h the left invariant 2-cocycle $\pi^*\Omega$ on G. Since Ω is non-degenerate, we see that an element X of $\mathfrak{g}$ belongs to $\mathfrak{b}$ if and only if $h(X,Y)=0$ for all $Y\in g$. Let S be a maximal connected semi-simple subgroup containing B.

In order to prove the lemma, we introduce a filtration in $C^*(G)$ by means of S. We denote by C^p the ideal in $C^*(G)$ generated by $N^p(G:S)$. The sequence $C^*(G)=C^0\supset C^1\supset\cdots\supset C^p\supset\cdots$ defines a filtration in $C^*(G)$. Let $Z^p{}_s$ be the set of all elements $a\in C^p$ such that $da\in C^{p+s}$, and put $dZ^{p-s}{}_s=D^p{}_s$. Then $Z^{p+1}{}_{s-1}+D^p{}_{s-1}$ is an ideal of $Z^p{}_s$. We denote by $E^p{}_s$ the factor algebra $Z^p{}_s/Z^{p+1}{}_{s-1}$ and by $\eta^p{}_s$ the natural projection from $Z^p{}_s$ onto $E^p{}_s$. Let $E^{q,p}{}_s$ be the subspace of $E^p{}_s$ consisting of all elements which are images of elements of degree $p+q$ in $Z^p{}_s$. As for $E^{q,p}{}_1$, it is known from a theorem of Koszul ([5], Theorem 15.2) that there is an isomorphism from $H^q(S)\otimes L^p(G:S)$ onto $E^{q,p}{}_1$, where $H^q(S)$ is the q-homogeneous part of the cohomology algebra $H^*(S)$. Since S is semi-simple, we have $H^1(S)=H^2(S)=\{0\}$. It follows that $E^{1,p}{}_1=E^{2,p}{}_1=\{0\}$, $0\leqq p$.

Since the form h is a cocycle, h belongs to $Z^0{}_s$ for any s. Since the degree of h is two, we have $\eta^0{}_1h\in E^{2,0}{}_1$. Hence we have $\eta^0{}_1h=0$, which shows that $h\in Z^1{}_0+D^0{}_0$ that is, h is cohomologous to an element $h'\in Z^1{}_0$. The form h' being a cocycle in $Z^1{}_0$, we have $h'\in Z^1{}_s$ for all s. From the facts that $E^{1,1}=\{0\}$ and that $\eta^1{}_1h'\in E^{1,1}{}_1$, we have $\eta^1{}_1h'=0$ and $h'\in Z^2{}_0+D^1{}_0$. Hence h' is cohomologous to an element $h''\in Z^2{}_0$. Since the degree of h'' is two, h'' is in $N^2(G:S)$. Moreover, h'' being a cocycle, we have $\theta(X)h''=\iota(X)dh''+d\iota(X)h''=0$ for all $X\in\mathfrak{s}$, where $\mathfrak{s}$ denotes the subalgebras of $\mathfrak{g}$ corresponding to S. Therefore h'' belongs to $L^2(G:S)$. It follows that the cocycle h is cohomologous to the cocycle h'' which is in $L^2(G:S)$, that is, $h-h''=da$ for a certain $a\in C^1(G)$.

Next we shall prove that h and h'' are cohomologous to each other in $L^*(G:B)$. For this purpose, it is sufficient to show that a is contained in $L^*(G:B)$. Since $B\subset S$, we have $L^*(G:B)\supset L^*(G:S)$, and so h'' and da are in $L^2(G:B)$. Hence we have $\theta(X)a=\iota(X)da+d\iota(X)a=0$ for all

[3] First the author dealt with the case where the isotopy group $B=\{e\}$. The generalization is due to Matsushima.

$X \in \mathfrak{b}$, that is, $a([X, Y]) = 0$ for all $X \in \mathfrak{b}$ and $Y \in \mathfrak{g}$. Since $\mathfrak{b}$ is semi-simple, the derived algebra $[\mathfrak{b}, \mathfrak{b}]$ of $\mathfrak{b}$ coincides with $\mathfrak{b}$. Therefore we have $\iota(X)a = 0$ for all $X \in \mathfrak{b}$, and so we have $a \in L^2(G:B)$.

From our assumption, the $2m$-cocycle h^m is not zero. Hence h^m is not cohomologous to zero in $L^*(G:B)$. This follows from our assumption that $H^{2m}(G/B) \neq \{0\}$ and from the fact that G is connected. Suppose that $\mathfrak{b}$ were not equal to $\mathfrak{s}$, and let X_0 be an element of $\mathfrak{s}$ not contained in $\mathfrak{b}$. Since $h'' \in L^*(G:S)$, we would have $(\iota(X_0)h'')(Y) = \frac{1}{2}h''(X_0, Y) = 0$ for all $Y \in \mathfrak{g}$ and accordingly $h''^m = 0$. On the other hand, h'' and h''^m are cohomologous to each other in $L^*(G:b)$. This is impossible and hence we have $\mathfrak{b} = \mathfrak{s}$, which implies $B = S$. Thus the proof is completed.

8. In this section we prepare two lemmas for the first theorem.

LEMMA 2. *Let G/B be a Kaehlerian homogeneous space of dimension $2m$. If B is a connected semi-simple subgroup, and if $H^{2m}(G/B) \neq \{0\}$, then the Ricci curvature r is zero.*

From our assumption that B is a connected semi-simple subgroup, G/B is a reductive homogeneous space; let $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ be an $\operatorname{ad} B$-stable decomposition. Let us consider the complexification $\mathfrak{m}^c$ of $\mathfrak{m}$, and let $\mathfrak{m}^+$ (resp. $\mathfrak{m}^-$) be the complex subspace spanned by all vectors $X - (-1)^{\frac{1}{2}} I_\circ X$ (resp. $X + (-1)^{\frac{1}{2}} I_\circ X$), $X \in \mathfrak{m}$. The space $\mathfrak{m}^+$ and $\mathfrak{m}^-$ are eigenspaces of $I_\circ$ belonging to the eigenvalues $(-1)^{\frac{1}{2}}$ and $-(-1)^{\frac{1}{2}}$ respectively. If $X \in \mathfrak{b}$, $(\operatorname{ad} X)_{\mathfrak{m}}$ commutes with $I_\circ$ and so leaves $\mathfrak{m}^+$ and $\mathfrak{m}^-$ stable respectively. Hence we have two representations of the subalgebra $\mathfrak{b}$ given by $X \to (\operatorname{ad} X)_{\mathfrak{m}^+}$ and $X \to (\operatorname{ad} X)_{\mathfrak{m}^-}$; these representations are mutually conjugate. Recalling that $(\operatorname{ad} X)_{\mathfrak{m}}$ is skew symmetric with respect to the inner product $g_\circ$ on $\mathfrak{m}$, we have $\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (\operatorname{ad} X)_{\mathfrak{m}} = 2(-1)^{\frac{1}{2}} \operatorname{tr}_{\mathfrak{m}^+} (\operatorname{ad} X)_{\mathfrak{m}^+}$ for all $X \in \mathfrak{b}$. Furthermore, since $\mathfrak{b}$ is semi-simple, we have $\operatorname{tr}_{\mathfrak{m}^+} (\operatorname{ad} X)_{\mathfrak{m}^+} = 0$ for all $X \in \mathfrak{b}$. Thus we have $\operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (\operatorname{ad} X)_{\mathfrak{m}} = 0$ for all $X \in \mathfrak{b}$, which implies

$$\psi_\circ(X, Y) = \operatorname{tr}_{\mathfrak{m}} I_\circ \cdot (\operatorname{ad} X)_{\mathfrak{m}} = 0$$

for all $X, Y \in \mathfrak{m}$. In virtue of (6.1), the Ricci form α is cohomologous to zero. On the other hand α is a harmonic form by (6.2). Accordingly we have $\alpha = 0$ by proposition (5.2), completing the proof.

LEMMA 3. *Let G/B be a Riemannian homogeneous space on which G acts effectively. If the restricted homogeneous holonomy group is irreducible and if the Ricci curvature is zero, then the group G is unimodular.*

Let us consider the left invariant 1-form t on G defined by $t(X) = \mathrm{tr}_{\mathfrak{g}}\, \mathrm{ad}\, X$ for all $X \in \mathfrak{g}$. Obviously t is also right invariant and we have $dt = 0$. Since G is effective on G/B, $\mathrm{ad}\, X$, $X \in \mathfrak{b}$, is skew symmetric with respect to an inner product of $\mathfrak{g}$ by the argument in **1**. Hence we have $t(X) = 0$ for all $X \in \mathfrak{b}$. These facts show that the 1-cocycle t is contained in $L^1(G/B)$, and there is a G-invariant 1-cocycle τ on G/B such that $\pi^*\tau = t$. We have $\Delta\tau = d\delta\tau + \delta d\tau = 0$, because $\delta\tau$ is a constant over G/B. Since the Ricci curvature is zero, we see that τ is a parallel field, on account of (5.1). As we assume that the restricted homogeneous holonomy group is irreducible, we can conclude that either t is zero or the dimension of G/B is equal to one. In the second case G is a 1-dimensional abelian group. In any case, the group G is unimodular. We have completed the proof.

9. We shall prove the following

THEOREM 1. *Let G/B be a Kaehlerian homogeneous space of dimension $2m$. If B is a connected semi-simple subgroup and if $H^{2m}(G/B) \neq \{0\}$, then the restricted homogeneous holonomy group reduces to the identity group.*

Since the Kaehlerian form Ω defines an invariant symplectic structure on G/B, B is a maximal connected semi-simple subgroup of G by Lemma 1. Let R be the radical of G, that is, the maximal connected solvable normal subgroup of G. Then by a well known theorem of Levi-Malcev, we have $G = B \cdot R$ and $B \cap R$ is a discrete normal subgroup, which we denote by D. Hence the solvable group R is transitive on G/B and the isotropy group of o is equal to D. We have a left invariant Kaehlerian structure on the group R which is locally isomorphic with given one on G/B by the projection from R onto G/B. By Lemma 2, the Ricci curvature of G/B is zero and accordingly the Ricci curvature of R is also zero. Therefore, in order to complete the proof, it is sufficient to prove the following

LEMMA 4. *Let G be a connected solvable Lie group. If the Ricci curvature of a left invariant Riemannian metric is zero, then the restricted homogeneous holonomy group is equal to $\{e\}$.*

We take the universal covering group of G, then this space has a left invariant Riemannian metric naturally induced by that of G and the projection is locally isometric. Therefore, for our purpose, we have only to prove that the homogeneous holonomy group reduces to $\{e\}$, when the group G is simply connected. Let $G = G_0 \times G_1 \times \cdots \times G_s$ be the canonical decom-

position with respect to the homogeneous holonomy group. Each component G_i is also a solvable Lie group and its Riemannian metric is left invariant. Moreover, the Ricci curvature r_i on G_i is equal to zero. We shall show that the subgroups G_i, $1 \leqq i \leqq s$ do not appear in the decomposition, which means that the homogeneous holonomy group of the Riemannian space G is equal to $\{e\}$.

Assume that, say, $\dim G_1 = n_1 > 0$. Since the space G_1 is irreducible and since the Ricci curvature r_1 is zero, the group G_1 is unimodular by Lemma 3 and then we have $H^{n_1}(G) \neq \{0\}$. Since the Lie algebra $\mathfrak{g}_1$ of G_1 is a non-zero solvable algebra, the dimension of the derived algebra $\mathfrak{g}_1'$ is less than that of $\mathfrak{g}_1$. It follows that $\dim H^1(G_1) = \dim \mathfrak{g}_1 - \dim \mathfrak{g}_1' \neq 0$. In virtue of (5.2), the dimension of $H^1(G_1)$ is equal to that of the space of all left invariant harmonic forms of degree 1. Therefore, there is a non-zero harmonic form of degree 1. Therefore, there is a non-zero harmonic form a. By proposition (5.1), a is a parallel field. Since the homogeneous holonomy group is irreducible, we have $\dim G_1 = 1$, which is impossible. Thereby we have proved the lemma and completed the proof of Theorem 1.

Now, we shall clarify the algebraic structure of solvable Lie groups G which admit a locally flat Riemannian connection. Since the curvature tensor R is zero, we have $[D_X, D_Y] = D_{[X,Y]}$ for all $X, Y \in \mathfrak{g}$ by (2.3). The correspondence $X \to D_X$ gives a representation of the Lie algebra $\mathfrak{g}$. By a well known theorem of Lie, the derived algebra of a linear solvable Lie algebra consists of nilpotent linear mappings. Therefore D is nipotent for all $X \in \mathfrak{g}'$, where $\mathfrak{g}'$ is the derived algebra of $\mathfrak{g}$. On the other hand, D_X is a skew symmetric linear mapping with respect to the inner product g by (2.2), and hence we have $D_X = 0$ for all $X \in \mathfrak{g}'$. If $X, Y \in \mathfrak{g}'$, we have $[X, Y] = D_X Y - D_Y X = 0$, which shows that $\mathfrak{g}'$ is abelian. Thus we have shown that the group G is meta-abelian. Let $\mathfrak{h}$ be the orthogonal complement of $\mathfrak{g}'$ with respect to the inner product g. If $X \in \mathfrak{h}$ and $Y \in \mathfrak{g}'$, we have $[X, Y] = D_X Y - D_Y X = D_X Y$. Since $\mathfrak{g}'$ is an ideal, we have $D_X Y \in \mathfrak{g}'$. Hence we see that $\mathfrak{g}'$ and accordingly $\mathfrak{h}$ are stable by D_X for all $X \in \mathfrak{h}$, and that $\operatorname{ad} X$ and D_X induce the same linear mapping on $\mathfrak{g}'$ for all $X \in \mathfrak{h}$. It follows that if $X, Y \in \mathfrak{h}$, $[X, Y] = D_X Y - D_Y X \in \mathfrak{h}$. On the other hand we have $[\mathfrak{h}, \mathfrak{h}] \subset \mathfrak{g}'$. According we have $[\mathfrak{h}, \mathfrak{h}] = 0$.

Now, let us assume that $\mathfrak{g}$ is nilpotent. Then $\operatorname{ad} X$ is nilpotent for all $X \in \mathfrak{g}$. If $X \in \mathfrak{h}$, the restriction on $\mathfrak{g}'$ of $\operatorname{ad} X$, which coincides with that of D_X, is simultaneously nilpotent and skew symmetric and accordingly is equal to zero. Hence we have $[\mathfrak{h}, \mathfrak{g}'] = 0$. After all we have proved that $\mathfrak{g}$ is abelian. From these considerations we have

THEOREM 2. *If a unimodular Lie group G admits a left invariant Kaehlerian structure, then the restricted homogeneous holonomy group is equal to $\{e\}$ and the group G is meta-abelian. Especially if the group G is nilpotent, then it must be abelian.*

If a Lie group G admits a left invariant Kaehlerian structure whose Ricci curvature is zero, then we have the same conclusion as above on account of Lemma 4.

10. We now prove the following

THEOREM 3. *Let G/B be a $2m$-dimensional Kaehlerian homogeneous space having the non-degenerate Ricci curvature. If G acts effectively on G/B and if $H^{2m}(G/B) \neq \{0\}$, then the group G is semi-simple.*

Since G is effective on G/B, the subgroup B is reductive in G by (1.1), and if $b \in B$, $\mathrm{ad}\, b$ is orthogonal with respect to a certain positive definite symmetric bilinear form on $\mathfrak{g}$. Let $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ be an $\mathrm{ad}\, B$-stable decomposition of $\mathfrak{g}$.

Since the Ricci curvature is non-degenerate, so is the Ricci form α. Hence we have $\alpha^m \neq 0$, which shows that α^m is not cohomologous to zero on account of our assumption that $H^{2m}(G/B) \neq \{0\}$. By (6.1), the cocycle α is cohomologous to the G-invariant cocycle ψ defined by

$$\psi_o(X, Y) = \mathrm{tr}_{\mathfrak{m}} I_o \cdot (\mathrm{ad}[X, Y]_{\mathfrak{b}})_{\mathfrak{m}}$$

for all $X, Y \in \mathfrak{m}$. Hence ψ^m, being cohomologous to α^m, is not cohomologous to zero, and a fortiori, ψ^m is not zero. Thus we see that ψ is non-degenerate, that is $\mathrm{tr}_{\mathfrak{m}} I_o \cdot (\mathrm{ad}[X, Y]_{\mathfrak{b}})_{\mathfrak{m}} = 0$ for all $Y \in \mathfrak{m}$, if and only if $X = 0$.

Let $\mathfrak{a}$ be an arbitrary abelian ideal of $\mathfrak{g}$. If $X \in \mathfrak{a}$, $\mathrm{ad}\, X$ is a nilpotent linear mapping. We can easily verify that $\mathfrak{a} \cap \mathfrak{b} = \{0\}$. In fact, if an element X is contained in $\mathfrak{a} \cap \mathfrak{b}$, $\mathrm{ad}\, X$ is simultaneously skew symmetric and nilpotent. Hence we have $\mathrm{ad}\, X = 0$ for all $X \in \mathfrak{a} \cap \mathfrak{b}$ which implies that $\mathfrak{a} \cap \mathfrak{b}$ is an ideal contained in the center of $\mathfrak{g}$. Since G is effective on G/B, the subalgebra $\mathfrak{b}$ cannot contain any ideal of $\mathfrak{g}$ except the zero ideal, and hence we have $\mathfrak{a} \cap \mathfrak{b} = \{0\}$. Since the subgroup B is reductive in G, we can take an $\mathrm{ad}\, B$-stable decomposition $\mathfrak{g} = \mathfrak{b} + \mathfrak{m}$ such that $\mathfrak{m}$ contains $\mathfrak{a}$. Let us apply the above consideration to this decomposition. If $X \in \mathfrak{a}$ and $Y \in \mathfrak{g}$, $[X, Y]$ belongs to $\mathfrak{a}$ and hence we have $[X, Y]_{\mathfrak{b}} = 0$. It follows that if $X \in \mathfrak{a}$, $\mathrm{tr}_{\mathfrak{m}} I_o \cdot (\mathrm{ad}[X, Y]_{\mathfrak{b}})_{\mathfrak{m}} = 0$ for all $Y \in \mathfrak{m}$, which shows that $\mathfrak{a} = \{0\}$.

Thus we have seen that any abelian ideal in $\mathfrak{g}$ reduces to $\{0\}$, and accordingly the algebra $\mathfrak{g}$ is semi-simple, which completes the proof.

NAGOYA UNIVERSITY.

REFERENCES.

[1] A. Borel, "Kaehlerian coset spaces of semi-simple Lie groups," *Proceedings of the National Academy of Science, U. S. A.*, vol. 40 (1954), pp. 1147-1151.

[2] E. Cartan, "Sur les domaines bornés homogènes de l'espace de n variables complexes," *Abh. Math. Seminar Hamburg*, vol. 11 (1935), pp. 116-162.

[3] G. de Rham, "Sur la réductibilité d'un espace de Riemann," *Comm. Math. Helv.*, vol. 26 (1952), pp. 328-344.

[4] ———, *Variétés Différentiables*, Hermann, Paris (1955).

[5] J. L. Koszul, "Homologie et cohomologie des algèbres de Lie," *Bulletin Soc. Math. France*, vol. 78 (1950), pp. 65-127.

[6] ———, "Sur la forme hermitienne canonique des espace homogènes complexes," *Canadian Journal of Mathematics*, vol. 7 (1955), pp. 562-576.

[7] A. Lichnerowicz, "Espaces homogènes kaehlériens," *Coll. Géom. Diff.* (Strasbourg, 1953), pp. 171-184.

[8] Y. Matsushima, "Sur les espaces homogènes kaehlériens d'un groupe de Lie réductif," *Nagoya Mathematical Journal*, vol. 11 (1957), pp. 53-60.

[9] K. Nomizu, "Invariant affine connections on homogeneous spaces," *American Journal of Mathematics*, vol. 76 (1954), pp. 33-65.

[10] ———, "Studies on Riemannian homogeneous spaces," *Nagoya Mathematical Journal*, vol. 9 (1955), pp. 43-56.

SINGULAR INTEGRAL OPERATORS AND DIFFERENTIAL EQUATIONS.* [1]

By A. P. Calderón and A. Zygmund.

1. Introduction. Let $P(u)$ be a linear partial differential operator with smooth coefficients and of homogeneous order m. Then $P = H\Lambda^m$ where Λ is a square root of the Laplacian (see definition [1] below) and H is a singular integral operator (see Theorem 7). This fact seems to call for a closer study of the properties of singular integral operators in their connection with the operator Λ and supplies the subject matter of the present paper.

Our results can be briefly summarized as follows. With each singular integral operator there is associated a function (its "symbol" in the terminology of Giraud and Mihlin) in a one-to-one fashion. This correspondence is linear and pseudo-multiplicative in the sense that, modulo a class of regular operators, singular integral operators can be multiplied (in the sense of operator composition) by simply multiplying their symbols. The regular operators in that class have the property of remaining bounded after being multiplied on the left or on the right by Λ. An algebraic formulation of these facts will be found in Theorem 6. The reader familiar with the work of Giraud, Mihlin and Tricomi [1a] will recognize the similarity of some of our results with theirs. The main distinctive feature is that we are concerned with the operator Λ which they do not consider, and that our operators act on L^p, $1 < p < \infty$, instead of on L^2 only. For many applications, though, it suffices to consider the case of L^2, and, in this respect and as far as mean convergence of the singular integrals goes, the paper is self-contained. To conclude these preliminary remarks, we want to stress the fact that many of the assumptions on which our results are obtained can be considerably relaxed. Since these improvements do not seem to be of particular relevance at the present time, we prefer not to burden the reader and postpone their discussion to another opportunity.

---

* Received June 12, 1957.

[1] This research was partly supported by the United States Air Force under contract No. AF18(600)-685 monitored by the Office of Scientific Research.

[1a] A description of the work of these authors can be found in the paper "Singular integral equations" by S. G. Mihlin, Uspekhi Matematicheskikh Nauk, No. 25 (1948), 29-112.

2. Definitions and notation. We will be concerned with functions defined in the k-dimensional Euclidean space E_k. Points in E_k will be denoted by $x=(x_1,\cdots,x_k)$, $y=(y_1,\cdots,y_k)$ etc. and we will use the following abbreviations $|x|=[\sum_1^k x_i^2]^{\frac{1}{2}}$, $\lambda x=(\lambda x_1,\cdots,\lambda x_k)$, $x'=x|x|^{-1}$, $x+y=(x_1+y_1,\cdots,x_k+y_k)$, $x\cdot y=\sum_1^k x_iy_i$. The sphere $|x|=1$ in E_k will be denoted by Σ, the element of surface area on Σ by $d\sigma$, and dx will stand for the volume element in E_k. By C_α, $\alpha\geqq 0$, we shall denote the class of complex valued continuous bounded functions on E_k with bounded continuous derivatives up to order $[\alpha]$ (integral part of α) and with derivatives of order $[\alpha]$ satisfying a (uniform) Hölder condition of order $\alpha-[\alpha]$. When dealing with functions depending on more than one argument, we will denote by C_α^∞ the class of functions in C_α which are in C^∞ with respect to the last argument and whose derivatives of all orders with respect to variables in the last argument are in C_α. Given a subclass of C_α or C_α^∞, we shall say that the subclass is uniform if the bounds and Hölder conditions on the functions and their derivatives are uniform in the subclass.

We shall also consider the class L_r^p of functions in $L^p(E_k)$ with derivatives up to order r in $L^p(E_k)$. The notion of derivative used here is that of Schwartz; that is, $g=\partial f/\partial x_i$ means $(f,\partial\phi/\partial x_i)=-(g,\phi)$ for every $\phi\in C^\infty$ vanishing outside a bounded set, where here, as in the rest of the paper, (f,g) stands for the integral of $f\bar{g}$ over E_k. By A and C we will denote constants, though they will not be necessarily the same in different occurrences.

3. In this section we shall establish some properties of expansions of functions in spherical harmonics. Let $Y_n(x')$ be a normalized real spherical harmonic of degree n, that is, such that

$$\int_\Sigma Y_n(x')^2 . d\sigma=1$$

and $Y_{nm}(x')$, $m=1,2,\cdots$, a complete orthogonal system of normalized harmonics of degree n. Our first objective is to obtain bounds for the $Y_n(x')$ and their successive derivatives. Consider first the case $k\geqq 3$. Then we have the formula (see [4])

$$(1)\qquad \delta_{nm}Y_m(x')=\tfrac{1}{2}\Gamma(\lambda)(n+\lambda)/\pi^{\lambda+1}\int_\Sigma P_n^\lambda(x'\cdot y')Y_n(y')\,d\sigma$$

where $\lambda=\frac{1}{2}(k-2)$, δ_{nm} is Kronecker's delta and $P_n^\lambda(t)$ is the ultraspherical polynomial defined by

$$(1-2wt+w^2)^{-\lambda}=\sum_0^\infty w^n P_n^\lambda(t). \tag{2}$$

For each z, the function $P_n^\lambda(x'\cdot z')$ is a spherical harmonic of degree n, whence, replacing in (1) and setting $x'=z'$, we obtain

$$P_n^\lambda(1)=\tfrac{1}{2}\Gamma(\lambda)(n+\lambda)/\pi^{\lambda+1}\int_\Sigma P_n(y'\cdot z')^2\,d\sigma.$$

On the other hand, from (2) it follows that

$$(1-w)^{-k+2}=\sum_0^\infty w^n P_n^\lambda(1),$$

which implies that $P_n^\lambda(1)$ is of the order n^{k-3} as $n\to\infty$. Hence

$$\int_\Sigma P_n^\lambda(y'\cdot z')^2\,d\sigma$$

is of order n^{k-4}, and Schwarz's inequality applied to (1) gives

$$|Y_n(x')|\leqq Cn^{\frac{1}{2}(k-2)}, \qquad n\geqq 1, \tag{3}$$

where C is a constant depending only on k. In order to estimate the derivatives of $Y_n(x')$, let $P_n(x)$ denote temporarily the solid harmonic coinciding with $Y_n(x')$ on Σ. Then, if S denotes the sphere $|x|\leqq 1$ and $\partial P_n/\partial\nu$ is the derivative of P_n in the direction of the outer normal to the boundary Σ of S, we have

$$\int_\Sigma P_n(\partial P_n/\partial\nu)\,d\sigma=\int_S|\operatorname{grad}P_n|^2\,dx.$$

Now P_n and $|\operatorname{grad}P_n|^2$ are homogeneous functions of degrees n and $2n-2$, respectively, and from this it follows readily that the two integrals are respectively equal to

$$n\int_\Sigma P_n^2\,d\sigma=n \text{ and } (2n+k-2)^{-1}\int_\Sigma|\operatorname{grad}P_n|^2\,d\sigma,$$

which implies that

$$\int_\Sigma|\partial P_n/\partial x_i|^2\,d\sigma\leqq Cn^2.$$

But $\partial P_n/\partial x_i$ is a homogeneous harmonic polynomial of degree $n-1$, and therefore we can write $\partial P_n/\partial x_i=\lambda P_{n-1}$, where P_{n-1} is a solid harmonic coinciding with a normalized spherical harmonic of degree $n-1$ on Σ, and $|\lambda|\leqq Cn$.

Now we write $Y_n(x')=|x|^{-n}P_n(x)$, and by differentiating and applying (3) and the formula above to the successive derivatives of P_n, we obtain

$$(4) \qquad | D_r Y_n(x') | \leqq C n^{\frac{1}{2}(k-2)+r}, \qquad |x| \geqq 1,$$

where $D_r Y_n$ denotes a derivative of Y_n of order r and C is a constant depending on r and k. If $k=2$, a normalized spherical harmonic is the real part of $\pi^{-\frac{1}{2}} e^{i\theta}(w\,|w|^{-1})^n$, where $w = x_1 + ix_2$ and θ is a real number. Clearly (3) still holds in this case and (4) is obtained by differentiation.

Our next step will be to establish the formula (8) for the coefficients of the expansion of a function in spherical harmonics.

Let $F(x) = F(x')$, $G(x) = G(x')$ be two homogeneous functions of degree zero, and let S_ϵ be the spherical shell between the spheres of radii 1 $1+\epsilon$. Since F and G are homogeneous of degree zero, their normal derivatives at points of the boundary of S_ϵ are zero. Consequently, if we apply Green's formula to the pair F, G, the surface integral vanishes and we obtain

$$\int_{S_\epsilon} F \Delta G \, dx = \int_{S_\epsilon} G \Delta F \, dx;$$

dividing by ϵ and letting ϵ tend to zero it follows that

$$\int_\Sigma F \Delta G \, d\sigma = \int_\Sigma G \Delta F \, d\sigma.$$

If we define now

$$(5) \qquad L(F) = |x|^2 \Delta F(x),$$

then, since $|x| = 1$ on Σ, it follows that

$$\int_\Sigma FL(G)\, d\sigma = \int_\Sigma GL(F)\, d\sigma.$$

But if F is homogeneous of degree zero, so is $L(F)$, and a repeated application of the last formula gives

$$(6) \qquad \int_\Sigma FL^r(G)\, d\sigma = \int_\Sigma GL^r(F)\, d\sigma$$

which holds, of course, if F and G have sufficiently many continuous derivatives in $|x| > 0$.

Let us consider now a spherical harmonic $Y_{nm}(x')$. Then $|x|^n Y_{nm}(x')$ is a solid harmonic and its Laplacian vanishes. Since the gradients of $Y_{nm}(x')$ and $|x|^n$ are mutually orthogonal, we have that

$$0 = \Delta[\,|x|^n Y_{nm}(x')] = |x|^n \Delta Y_{nm} + n(n+k-2)\,|x|^{n-2} Y_{nm};$$

whence, we obtain

$$(7) \qquad L[Y_{nm}(x')] = -n(n+k-2)\, Y_{nm}(x').$$

Let now $F(x')$ be a homogeneous function of degree zero and let

$$F(x') = a_0 + \sum_{n \geqq 1} a_{nm} Y_{nm}(x')$$

be its expansion in spherical harmonics. Then

$$a_{nm} = \int_{\Sigma} F(x') Y_{nm}(x') \, d\sigma, \qquad n \geqq 1,$$

and an application of (7) and (6) to the last integral gives

$$(8) \qquad a_{nm} = (-1)^r n^{-r} (n+k-2)^{-r} \int_{\Sigma} L^r(F) Y_{nm}(x') \, d\sigma, \qquad n \geqq 1.$$

Now we shall compute compute the Fourier transforms of homogeneous functions coinciding with a normalized spherical harmonic on Σ. Let us write

$$(9) \qquad \begin{aligned} Y_{nm}(\epsilon, \delta, x) &= \begin{cases} Y_{nm}(x') \, | x |^{-k} & \text{if } \epsilon \leqq | x | \leqq \delta, \\ 0 & \text{otherwise}, \end{cases} \\ Y_{nm}(\epsilon, x) &= \begin{cases} Y_{nm}(x') \, | x |^{-k} & \text{if } \epsilon \leqq | x |, \\ 0 & \text{otherwise}. \end{cases} \end{aligned}$$

Then

$$\hat{Y}_{nm}(\epsilon, \delta, x) = \int_{\epsilon \leqq |y| \leqq \delta} e^{i(x \cdot y)} Y_{nm}(y') \, | y |^{-k} \, dy$$

Now we set $r = | x |$, $\rho = | y |$ and denote by γ the angle between x and y, and the integral above becomes

$$\begin{aligned} &\int e^{ir\rho \cos \gamma} Y_{nm}(y') \, | y |^{-k} \, dy \\ (10) \qquad &= \int_{\epsilon}^{\delta} d\rho / \rho \int_{\Sigma} e^{ir\rho \cos \gamma} Y_{nm}(y') \, d\sigma = \int_{\epsilon r}^{\delta r} ds/s \int_{\Sigma} e^{is \cos \gamma} Y_{nm}(y') \, d\sigma, \end{aligned}$$

and since the integral of Y_{nm} over Σ is zero, the last integral can be written as

$$\begin{aligned} &\int_{\epsilon r}^{\delta r} ds/s \int_{\Sigma} (e^{is \cos \gamma} - e^{-s}) Y_{nm}(y') \, d\sigma \\ &\qquad = \int_{\Sigma} Y_{nm}(y') \left[\int_{\epsilon r}^{\delta r} (e^{is \cos \gamma} - e^{-s}) / s \, ds \right] d\sigma. \end{aligned}$$

Now the inner integral can be estimated readily by integrating between ϵr and 1, and 1 and δr, and one verifies that it is dominated in absolute value by $\log C / | \cos \gamma |$ and that it converges as $\epsilon \to 0$ and $\delta \to \infty$. Hence, applying Schwarz's inequality to the last integral, we obtain

$$(11) \qquad | \hat{Y}_{nm}(\epsilon, \delta, x) | \leqq C, \qquad | \hat{Y}_{nm}(\epsilon, x) | \leqq C,$$

where C depends only on k. Further, as $\epsilon \to 0$ and $\delta \to \infty$, both functions converge to the same limit which we shall denote by $\hat{Y}_{nm}(x)$.

Now we wish to obtain an explicit expression for $\hat{Y}_{nm}(x)$ (see also [2]). For this purpose, let us revert to (10) and assume first that $k \geqq 3$. Then from the expansion

$$e^{is\cos\gamma} = 2^\lambda \Gamma(\lambda) \sum_{n=0}^{\infty} (n+\lambda) i^n J_{n+\lambda}(s)/s^\lambda P_n{}^\lambda(\cos\gamma), \qquad \lambda = \tfrac{1}{2}(k-2),$$

where J_k is Bessel's function of order k and which converges uniformly in γ and s for s in any finite interval (see [5], p. 368), and from (1), we obtain

$$\hat{Y}_{nm}(\epsilon, \delta, x) = i^n (2\pi)^{k/2} \left[\int_{\epsilon r}^{\delta r} J_{n+\lambda}(s)/s^{1+\lambda}\, ds \right] Y_{nm}(x').$$

Letting ϵ tend to zero and δ tend to infinity and on account of the formula (see [5], p. 391)

$$\int_0^\infty J_{n+\lambda}(s)/s^{1+\lambda}\, ds = 2^{-\frac{1}{2}k} \Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[n+k]), \tag{12}$$

we obtain

$$\hat{Y}_{nm}(x) = i^n \pi^{\frac{1}{2}k} \Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[k+n]) Y_{nm}(x'). \tag{13}$$

In the case $k=2$, we write $y_1 = \rho\cos\phi$, $y_2 = \rho\sin\phi$, $x_1 = r\cos\theta$, $x_2 = r\sin\theta$, and the inner integral on the right-hand side of (10) becomes

$$\int_0^{2\pi} e^{is\cos(\phi-\theta)} \cos n(\phi-\phi_0)\, d\phi = 2\pi J_n(s) i^n \cos n(\theta-\phi_0),$$

and integrating and applying (12) we obtain (13).

4. In this section we shall consider the Riesz transforms and the operator Λ.

The Riesz transforms are defined as follows. Let

$$R_{m\epsilon}(f) = -i\pi^{-\frac{1}{2}(k+1)} \Gamma[\tfrac{1}{2}(k+1)] \int_{\epsilon<|x-y|} (x_m - y_m)/|x-y|^{k+1} f(y)\, dy. \tag{14}$$

Then

$$R_m(f) = \operatorname*{l.i.m.}_{\epsilon\to 0} R_{m\epsilon}(f). \tag{15}$$

THEOREM 1. *If $f \in L^p$, $1<p<\infty$, the limit on the right of* (15) *exists as a limit in the mean of order p, and*

$$\| R_{m\epsilon} f \|_p \leqq A_p \| f \|_p, \tag{16}$$

where A_p depends only on p and k, and $\| f \|_p$ is the L^p-norm of f. If $f \in L_r{}^p$, $r \geqq 1$, then $R_m f \in L_r{}^p$

$$(\partial/\partial x_n)R_m = R_m(\partial/\partial x_n), \tag{17}$$

$$R_m(\partial/\partial x_n) = R_n(\partial/\partial x_m), \tag{18}$$

where $\partial/\partial x_n$ is the operator differentiation with respect to x_n.

Finally, R_m is selfadjoint in the sense that if $f \in L^p$ and $g \in L^q$, $1 < p < \infty$, $p^{-1} + q^{-1} = 1$, then $(R_m f, g) = (f, R_m g)$, and

$$\sum_{m=1}^{k} R_m^2 = I, \qquad R_m R_n = R_n R_m, \tag{19}$$

where I is the identity operator.

In order to establish these results it will be convenient to prove first the following

LEMMA 1. *Let $f \in L_r^p$, then there exists a sequence of functions f_n in C^∞, each vanishing outside a bounded set, such that $\| f_n - f \|_p \to 0$ and $\| D_j f_n - D_j f \|_p \to 0$ for each derivative $D_j f$ of f of order $j \leqq r$.*

Let $\phi(x)$ and $\psi(x)$ be two functions in C^∞ vanishing outside a bounded set. Assume that $\phi(x) = 1$ in a neighborhood of $x = 0$ and that

$$\int_{E_k} \psi(x)\, dx = 1.$$

Let $\phi_n = \phi(x/n)$ and $\psi_n = n^k \psi(nx)$. Then, if $\psi_n * f$ denotes the convolution of ψ_n and f, we have that

$$\| \psi_n * f - f \|_p \to 0 \tag{20}$$

and

$$\| \psi_n * D_j f - D_j f \|_p \to 0$$

as $n \to \infty$. Now, since ψ_n is in C^∞ and vanishes outside a bounded set, from the definition of derivatives of functions in L_r^p (see Section 2) and by differentiation under the integral sign, we obtain that

$$D_j(\psi_n * f) = (D_j \psi_n) * f = \psi_n * D_j f.$$

Consequently,

$$\| D_j(\psi_n * f) - D_j f \|_p \to 0. \tag{21}$$

Now since $\phi_n(x) \to 1$ for each x, and since each derivative of $\phi_n(x)$ converges uniformly to zero as $n \to \infty$, we have that

$$\begin{aligned} &\| D_j[\phi_n(\psi_n * f)] - \phi_n D_j(\psi_n * f) \|_p \to 0 \\ &\| \phi_n D_j(\psi_n * f) - D_j(\psi_n * f) \|_p \to 0. \end{aligned} \tag{22}$$

If we set now $f_n = \phi_n(\psi_n * f)$, the desired result follows from (20), (21) and (22).

We revert now to the proof of Theorem 1. If $f \in L^2$ the fact that $R_{m\epsilon}(f)$ converges in the mean of order 2 follows by taking Fourier transforms in (14). In the previous section, we showed that the Fourier transform of the kernel of the integral operator (14)[2] converges boundedly to $x_m|x|^{-1}$ as $\epsilon \to 0$, and this clearly implies the convergence of $R_{m\epsilon}(f)$ and (16).

In the general case, the convergence in the mean of $R_{m\epsilon}(f)$ and (16) follows from Theorem 1 in [3] (see also the remark on page 306 of the same paper).

In order to show that $R_m(f)$ belongs to $L_r{}^p$ if f does, it will be sufficient to consider the case $r = 1$; the general case will follow from (17).

Let $f \in L_1{}^p$ and let f_n be a sequence of functions as in the preceding lemma. Then by differentiating under the integral sign, we obtain

$$(\partial/\partial x_l) R_{m\epsilon} f_n = R_{m\epsilon}(\partial/\partial x_l) f_n,$$

and, if g is in C^∞ and vanishes outside a bounded set,

$$(g, R_{m\epsilon}(\partial/\partial x_l) f_n) = (g, (\partial/\partial x_l) R_{m\epsilon} f_n) = -((\partial/\partial x_l) g, R_{m\epsilon} f_n)$$

and letting first ϵ tend to zero and then n tend to infinity, on account of (16) we obtain

$$(g, R_m(\partial/\partial x_l) f) = -((\partial/\partial x_l) g, R_m f),$$

which shows that $R_m f \in L_1{}^p$ and that (17) holds.

In order to establish (18), we observe that, for every g in C^∞ vanishing outside a bounded set, we have $R_m \partial g/\partial x_l = R_l \partial g/\partial x_m$ (as one readily sees by taking Fourier transforms), and replacing g by the f_n of Lemma 1 and passing to the limit, we obtain $R_m \partial f/\partial x_n = R_n \partial f/\partial x_m$ for every f in $L_r{}^p$, $r \geqq 1$.

Finally, if f and g are bounded and vanish outside a bounded set, we have $(R_m f, g) = (f, R_m g)$ by interchanging the order of integration, and

$$\sum_{m=1}^{k} R_m{}^2(f) = f, \qquad R_m R_n(f) = R_n R_m(f)$$

by taking Fourier transforms, whence the general case follows from the continuity of R_m in L^p, $1 < p < \infty$.

Definition 1. Let $f \in L_r{}^p$, $r \geqq 1$, $1 < p < \infty$. Then

$$\Lambda f = i \sum_1^k R_m \partial f/\partial x_m = i \sum_1^k (\partial/\partial x_m) R_m f.$$

---

[2] Observe that this kernel coincides, except for a numerical factor, with one of the functions $Y_{1,m}(\epsilon, x)$ in (9).

COROLLARY. *If $f \in L_r^p$, $r \geqq 1$ then $\Lambda f \in L_{r-1}^p$ and*

$$i\partial f/\partial x_n = R_n \Lambda f = \Lambda R_n f. \tag{23}$$

If $f \in L_r^p$, $r \geqq 2$ then

$$\Delta' = \sum_1^k \partial^2 f/dx_m^2 = -\Lambda^2 f. \tag{24}$$

The first assertion follows from the definition of Λ and the fact that the operators R_m preserve the classes L_r^p. The formulas (23) and (24) are obtained from the definition of Λ by using (18) and (19).

5. We proceed to present the main results of the paper. We begin with

THEOREM 2. *Let $h(x,z)$; $x, z \in E_k$, be a function in C_β^∞, $\beta \geqq 0$, homogeneous of degree $-k$ in z, that is, such that $h(x, \lambda z) = \lambda^{-k} h(x,z)$ for every $\lambda > 0$, and assume that $\int_\Sigma h(x,z)\,d\sigma = 0$ for every x, where Σ is the sphere $|z| = 1$. Let $a(x)$ be a function in C_β, and consider the operator*

$$H_\epsilon f = a(x) f(x) + \int_{|x-y|>\epsilon} h(x, x-y) f(y)\,dy \tag{25}$$

and its adjoint

$$H_\epsilon^* f = \bar{a}(x) f(x) + \int_{|x-y|>\epsilon} \bar{h}(y, y-x) f(y)\,dy. \tag{26}$$

Then

i) *H_ϵ and H_ϵ^* are defined for $f \in L^p$, $1 < p < \infty$ and as $\epsilon \to 0$, $H_\epsilon(f)$ and $H_\epsilon^*(f)$ converge in the mean of order p. If $H(f)$ and $H^*(f)$ denote their respective limits, we have*

$$\begin{aligned} \| Hf \|_p &\leqq \| f \|_p A_p \sup_{|z|=1} (|a(x)| + |h(x,z)|), \\ \| H^* f \|_p &\leqq \| f \|_p A_q \sup_{|z|=1} (|a(x)| + |h(x,z)|), \end{aligned} \tag{27}$$

where $p^{-1} + q^{-1} = 1$ and A_p depends only on p and k.

ii) *if $f \in L_r^p$, $1 < p < \infty$, with $r \leqq \beta$, then Hf and H^*f belong to L_r^p,*

iii) *if $f \in L^p$, $1 < p < \infty$, and is Hölder-continuous of order α, $0 < \alpha < \beta$, Hf and H^*f are Hölder continuous of the same order.*

Part of i) concerning the operators H_ϵ and H was proved in [3], Theorem 2. The estimate of $\| Hf \|_p$, which also holds for $\| H_\epsilon f \|_p$, is not given explicitly there but is contained in the proof of the theorem. We shall therefore concentrate in the case $p = 2$. We begin with

LEMMA 2. *Let*

$$T_{nm\epsilon}f = \int_{|x-y|>\epsilon} Y_{nm}(\epsilon, x-y) f(y)\,dy, \tag{28}$$

where $Y_{nm}(\epsilon, x)$ is the function defined in (9). *Then if $f \in L^p$, $1 < p < \infty$, there is a constant A_p depending on p and k such that*

$$\| T_{nm\epsilon}f \|_p \leqq A_p \| f \|_p, \tag{29}$$

and as $\epsilon \to 0$, $T_{nm\epsilon}f$ converges in the mean of order p to a limit $T_{nm}f$. If $f \in L_r^p$, then $T_{nm}f \in L_r^p$. The operators T_{nm} commute with the R_m of Theorem 1 *and when acting on L_r^p, they also commute with the $\partial/\partial x_n$.*

The proof of this lemma proceeds as that of Theorem 1 and we need not repeat it here.

Now we revert to the operator H_ϵ. Let us expand the function $h(x, z)$ in spherical harmonics

$$h(x, z) = \Sigma a_{nm}(x) Y_{nm}(z') \,|\, z \,|^{-k}, \tag{31}$$

where the $a_{nm}(x)$ can be calculated by means of formula (8) after replacing F by h. Since, for each n, the number of distinct spherical harmonics Y_{nm} is of the order n^{k-2} and since, according to (3), Y_{nm} has a bound of the order $n^{\frac{1}{2}(k-2)}$, it follows from the formula (8), by choosing r sufficiently large, that the series of absolute values of the terms of the series above is dominated by a multiple of $|\, z \,|^{-k}$. Consequently, given $f \in L^p$, we can replace h by the series in (25) and (26) and integrate term by term obtaining

$$H_\epsilon f = a(x) f + \Sigma a_{nm}(x) T_{nm\epsilon} f, \qquad H_\epsilon^* f = \bar{a}(x) f + \Sigma(-1)^n T_{nm\epsilon}(\bar{a}_{nm} f). \tag{32}$$

Now the $a_{nm}(x)$ are dominated in absolute value by the terms of a convergent numerical series, and according to (29), the $T_{nm\epsilon}f$ are bounded in norm and converge in the mean as $\epsilon \to 0$. Hence $H_\epsilon f$ converges in the mean. Similarly, the functions $T_{nm\epsilon}(\bar{a}_{nm} f)$ converge in the mean and their norms are dominated by the terms of a convergent numerical series, which implies that $H_\epsilon^* f$ also converges.

Passing to the limit we obtain

$$Hf = a(x) f + \Sigma a_{nm}(x) T_{nm} f, \qquad H^* f = \bar{a}(x) f + \Sigma(-1)^n T_{nm}(\bar{a}_{nm} f), \tag{33}$$

the series converging in the mean of order p. If f and g vanish outside a bounded set and are bounded, from absolute integrability, it follows that $(H_\epsilon f, g) = (f, H_\epsilon^* g)$ and from the continuity of the operators H_ϵ and H_ϵ^* in every L^p, $1 < p < \infty$, we obtain $(H_\epsilon f, g) = (f, H_\epsilon^* g)$ for $f \in L^p$ and $g \in L^q$, $p^{-1} + q^{-1} = 1$, which justifies the assertion that H_ϵ^* is the adjoint of H_ϵ.

By a passage to the limit we obtain that also H^* is the adjoint of H.

Our next step will be establishing (27) in the case $p=2$. In the first place, we have that

$$|a(x)|^2+\Sigma|a_{nm}(x)|^2 \leqq \sup_x [|a(x)|^2+\int_{|z|=1}|h(x,z)|^2 d\sigma]=C^2,$$

and from (33) and Schwarz's inequality, we obtain

$$|Hf|^2 \leqq C^2[|f|^2+\Sigma|T_{nm}f|^2].$$

Integrating and applying Plancherel's theorem to the right hand side, we obtain (see formula (13))

$$\|Hf\|_2{}^2 \leqq C^2\int_{E_k}[1+\Sigma\pi^k\{\Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[k+n])\}^2 Y_{nm}(x')^2]|\hat{f}(x)|^2\,dx.$$

Now the sum of the squares of the spherical harmonics of a given degree n is a constant equal to the number of such harmonics divided by the area of Σ (see [1], p. 242). Since this number is of the order n^{k-2}, the series in the last integral is absolutely convergent and represents a constant, and we obtain

$$\|H_f\|_2{}^2 \leqq C^2A_2{}^2\|\hat{f}\|_2{}^2=C^2A_2{}^2\|f\|_2{}^2,$$

where $A_2{}^2$ is the value of the series, which is the first inequality in (27). The second is obtained from the fact that H^* is the adjoint of H.

We turn now to the proof of ii). Since the $a_{nm}(x)$ can be calculated by means of formula (8), replacing the function F there by $h(x,z)$, it follows readily by choosing r sufficiently large, that the $a_{nm}(x)$ and their derivatives of order less than or equal to β are dominated in absolute value by the terms of a convergent numerical series. Now if $f\in L_r{}^p$, then $T_{nm}f$ and $T_{nm}(a_{nm}f)$ belong to $L_r{}^p$, and from (29) it follows that the series in (33) can be differentiated term by term, which establishes ii).

In order to establish iii), we shall first investigate the Hölder continuity of $T_{nm}f$. Write $h(x)=Y_{nm}(x')|x|^{-k}$ and let S be any set contained in a sphere of radius ρ with center at x. Then if $f(x)$ is Hölder continuous of order α, $0<\alpha<1$, and $|f(x_1)-f(x_2)|\leqq A|x_1-x_2|^\alpha$, inequality (3) gives

$$(34)\qquad \left|\int_S h(x-y)[f(y)-f(x)]dy\right| \leqq \int_{|x-y|\leqq\rho} CAn^{\frac{1}{2}(k-2)}|x-y|^{-k+\alpha}dy = C/\alpha\, An^{\frac{1}{2}(k-2)}\rho^\alpha.$$

In particular, we have

$$(35)\qquad \left|\int_{|x-y|\leqq\rho} h(x-y)f(y)dy\right| \leqq \left|\int_{|x-y|\leqq\rho} h(x-y)[f(y)-f(x)]dy\right| \leqq C/\alpha\, An^{\frac{1}{2}(k-2)}\rho^\alpha.$$

Let now x_1 and x_2 be two points. Set $\rho = 2\,|\,x_1 - x_2\,|$ and write

$$(T_{nm}f)(x_1) - (T_{nm}f)(x_2)$$

$$= \int_{|x_1-y|\leqq\rho} h(x_1 - y)f(y)\,dy + \int_{|x_1-y|\geqq\rho} h(x_1 - y)[f(y) - f(x_2)]\,dy$$

$$- \int_{|x_1-y|\leqq\rho} h(x_2 - y)[f(y) - f(x_2)]\,dy + \int_{|x_1-y|\geqq\rho} h(x_2 - y)[f(y) - f(x_2)]\,dy,$$

where the integrals over $|\,y - x_1\,| \geqq \rho$ are understood as the limit as $R \to \infty$ of the integrals extended over $\rho \leqq |\,y - x_1\,| \leqq R$. Then from (34) and (25), we obtain

$$|(T_{nm}f)(x_1) - (T_{nm}f)(x_2)| \leqq C/\alpha\, A n^{\frac{1}{2}(k-2)}\rho^{\alpha}$$
$$+ \int_{|x_1-y|\geqq\rho} |\,h(x_1 - h) - h(x_2 - y)\,|\,|\,f(y) - f(x_2)\,|\,dy.$$

Now according to (4), $|\,h(x_1 - y) - h(x_2 - y)| \leqq Cn^{k/2}\,|\,x_1 - x_2\,|\,|\,x_1 - y\,|^{-k-1}$ in $|\,x_1 - y\,| \geqq \rho$, and since $|\,f(y) - f(x_2)\,| \leqq A\,|\,y - x_2\,|^{\alpha}$ and $|\,y - x_2\,| \leqq 2\,|\,y - x_1\,|$ in $|\,x_1 - y\,| \geqq \rho$, it follows that

$$|(T_{nm}f)(x_1) - (T_{nm}f)(x_2)| \leqq C/\alpha\, A n^{\frac{1}{2}(k-2)}\rho^{\alpha}$$
$$(36) \qquad + CAn^{k/2}\,|\,x_1 - x_2\,| \int_{\rho}^{\infty} s^{\alpha-2}\,ds \leqq [1/\alpha + 1/(1-\alpha)]CAn^{k/2}\,|x_1 - x_2|^{\alpha},$$

where the constant C in the last expression depends only on k. Further, since $\|\,T_{nm}f\,\|_p$ is bounded, as is readily verified, (36) implies that $(T_{nm}f)(x)$ has a bound of the order $n^{k/2}$. Now we can estimate $(Hf)(x_1) - (Hf)(x_2)$ from the series in (33). To obtain the desired result, it suffices to observe that, for every r, the functions $a_{nm}(x)n^r$ are uniformly bounded and uniformly Hölder continuous. This follows from formula (8) and allows us to estimate the preceding difference by estimating the corresponding differences of the terms of the series. The Hölder continuity of H^*f is established by a similar argument.

Remark. Infinite differentiability of $h(x, z)$ with respect to z is not indispensable for the validity of the preceding theorem, and, indeed, the argument used in its proof remains valid under weaker assumptions.

Another fact worth mentioning is this. Not only do the functions $H_\epsilon f$ and $H_\epsilon^* f$ converge in the mean of order p if f is in L^p, $1 < p < \infty$, but they converge pointwise almost everywhere and are dominated in absolute value by functions in L^p. For $H_\epsilon f$, this result is contained in Theorem 2 of [3]. The result for $H_\epsilon^* f$ can be obtained by applying Theorem 1 in [3] [3] to each

[3] See also the remark on page 306 of the same paper.

of the terms of the expansion in (33) after observing that the $a_{nm}(x)$ are dominated in absolute value by the terms of a convergent numerical series.

Definition 2. A singular integral operator of type C_β^∞ is an operator such as the H of Theorem 2. The symbol of the operator H is the function

$$\sigma(H) = a(x) + \Sigma a_{nm}(x)\gamma_n Y_{nm}(z'), \tag{37}$$

where $a(x)$ is the function in (25), *the $a_{nm}(x)$ are the functions in* (31), *and*

$$\gamma_n = i^n \pi^{k/2}\Gamma(\tfrac{1}{2}n)/\Gamma(\tfrac{1}{2}[n+k]). \tag{38}$$

The reader will notice that, on account of (13) the summation sign in (37) represents in a sense the Fourier transform of $h(x,z)$ with respect to z. This fact could be used in defining the symbol $\sigma(H)$ of H, but in the present set-up we find the preceding definition more convenient.

THEOREM 3. *If H is a singular integral operator of type C_β^∞ its symbol is a homogeneous function of degree zero with respect to z and in C_β^∞ in $|z| \geqq 1$. Conversely, every function of x and z which is homogeneous of degree zero with respect to z and belongs to C_β^∞ in $|z| \geqq 1$ is the symbol of a unique operator of type C_β^∞. If M is a bound for the absolute value of $\sigma(H)$ and its derivatives with respect to the coordinates of z in $|z| \geqq 1$ of order $2k$, then*

$$\| Hf \|_p \leqq MA_p \| f \|_p \tag{39}$$

where A_p depends only on p and k.

According to formula (8), we have

$$\begin{aligned} a_{nm}(x) &= (-1)^r n^{-r}(n+k-2)^{-r} \int_\Sigma L^r[h(x,z')]Y_{nm}(z')d\sigma, \\ a_{nm}(x) &= (-1)^r \gamma_n^{-1} n^{-r}(n+k-2)^{-r} \int_\Sigma L^r[\sigma(H)(x,z')]Y_{nm}(z')d\sigma, \end{aligned} \tag{40}$$

where L is the operator defined in (5) and x is regarded as a parameter. From this representation it follows readily that, if $h(x,z)$ or $\sigma(H)(x,z)$ belongs to C_β^∞ in $|z| \geqq 1$, then, for each r, the functions $a_{nm}(x)n^r$ are uniformly in C_β. Conversely, if the latter holds, by taking (4) into account and differentiating the series (31) and (37) term by term, we obtain that both $h(x,z)$ and $\sigma(H)(x,z)$ belong to C_β^∞ in $|z| \geqq 1$.

In order to establish (39) we just set $r = k$ in the last formula and obtain $|a_{nm}(x)| \leqq CMn^{-\frac{3}{2}k}$ where C is a constant depending only on k.

This combined with (3), (31) and the fact that the number of distinct

spherical harmonics of degree n is of the order n^{k-2} yields $|h(x,z)| \leqq CM$, where again C depends only on k. But on account of (27), this implies (39).

Definition 3. Let H, H_1 and H_2 be singular integral operators of type C_β^∞. We define $H^\#$ and $H_1 \circ H_2$ by the formulas

$$\sigma(H^\#) = \bar{\sigma}(H), \qquad \sigma(H_1 \circ H_2) = \sigma(H_1)\sigma(H_2),$$

where $\bar{\sigma}(H)$ is the complex conjugate of $\sigma(H)$.

THEOREM 4. *If the symbols of H, H_1 and H_2 are independent of x, then $H^\# = H^*$, $H_1 \circ H_2 = H_1 H_2 = H_2 H_1$ where $H_1 H_2$ is the composition product of H_1 and H_2.*

Let $f(x)$ be bounded and vanish outside a bounded set and let $\hat{f}$ be its Fourier transform. Then according to (32), we have $H_\epsilon f = af + \Sigma a_{nm} T_{nm\epsilon} f$, where a and a_{nm} are the same as those in (37) and are therefore assumed to be independent of x. Taking Fourier transforms and letting ϵ tend to zero, we obtain on account of (13)

$$(Hf)^\wedge = a\hat{f}(z) + \Sigma a_{nm}\gamma_n Y_{nm}(z')\hat{f}(z);$$

that is, $(Hf)^\wedge = \sigma(H)\hat{f}$, whence

$$(H^* f)^\wedge = \bar{\sigma}(H)\hat{f} = (H^\# f)^\wedge, \qquad [(H_1 \circ H_2)f]^\wedge = \sigma(H_1)\sigma(H_2)\hat{f} = (H_1 H_2 f)^\wedge,$$

which implies that $H^* f = H^\# f$ and $(H_1 \circ H_2)f = H_1 H_2 f$. From this and the continuity of H in L^p, the desired result follows.

COROLLARY. *If the symbol of the singular integral operator H is independent of x and does not vanish, then H has an inverse and the inverse is also a singular integral operator.*

Clearly the operator H_1 defined by $\sigma(H_1) = \sigma(H)^{-1}$ is an inverse of H.

The following theorem deals with the relationship between H^* and $H^\#$, and $H_1 H_2$ and $H_1 \circ H_2$ in the general case.

THEOREM 5. *Let H be an operator of type C_β^∞ with $\beta > 1$. Let M be a bound for $\sigma(H)(x,z)$ and its derivatives with respect to coordinates of z of order $2k$, the first derivatives of these with respect to the coordinates of x, and the Hölder constants of the latter. Then for every $f \in L_1^p$, $1 < p < \infty$, we have*

$$(41) \qquad \begin{aligned} &\|(H\Lambda - \Lambda H)f\|_p \leqq A_p M \|f\|_p, \quad \|(H^*\Lambda - \Lambda H^*)f\|_p \leqq A_p M \|f\|_p, \\ &\|(H^* - H^\#)\Lambda f\|_p \leqq A_p M \|f\|_p, \quad \|\Lambda(H^* - H^\#)f\|_p \leqq A_p M \|f\|_p. \end{aligned}$$

where A_p depends only on p, k and β. Further, if H_1 and H_2 are two operators in C_β^∞ and $f \in L_1^p$ then

$$(42) \qquad \begin{aligned} &\| (H_1 \circ H_2 - H_1 H_2) \Lambda f \|_p \leqq A_p M_1 M_2 \| f \|_p, \\ &\| \Lambda (H_1 \circ H_2 - H_1 H_2) f \|_p \leqq A_p M_1 M_2 \| f \|_p, \end{aligned}$$

where, again, A_p depends only on p, k and β and M_1 and M_2 are defined as above.

Let $c(x)$ be a function in C_β, T a singular integral operator with symbol independent of x, and f a function in C^∞ and vanishing outside a a bounded set. Denote by $Y(z)$ the kernel of the operator T, and consider the expression

$$(43) \qquad (cT - Tc) f_{x_i} = \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} [c(x) - c(y)] Y(x-y) f_{y_i} \, dy,$$

where f_{x_i} stands for $\partial f / \partial x_i$. Since $c(x) \in C_\beta$, $\beta > 1$, if $0 < \alpha \leqq \beta - [\beta]$, and $\alpha \leqq 1$, we have

$$| c_{x_j}(x) - c_{x_j}(y) | \leqq A \, | x - y |^\alpha,$$
$$c(x) - c(y) = \sum_j (x_j - y_j) c_{x_j}(x) + b(x,y),$$

where $| b(x,y) | \leqq kA \, | x - y |^{1+\alpha}$. Now we replace this expression in the integral in (43) and integrate by parts, obtaining

$$(44) \qquad \begin{aligned} &\int_{|x-y|>\epsilon} Y(x-y) c_{x_i}(y) f(y) \, dy \\ &+ \int_{\epsilon<|x-y|\leqq 1} \sum_j (x_j - y_j) c_{x_j}(x) Y_{x_i}(x-y) f(y) \, dy \\ &+ \int_{|x-y|>1} [c(x) - c(y)] Y_{x_i}(x-y) f(y) \, dy \\ &+ \int_{\epsilon<|x-y|\leqq 1} b(x,y) Y_{x_i}(x-y) f(y) \, dy \\ &+ \int_{|x-y|=\epsilon} [c(x) - c(y)] Y(x-y) f(y) \gamma_i \, d\sigma, \end{aligned}$$

where the last integral is extended over the surface of the sphere $| x - y | = \epsilon$ and γ_i is the i-th direction cosine of the normal to the spherical surface. Denote now by N_1 a bound for $| c(x) |$, $| c_{x_j} |$ and the Hölder constants for the derivatives c_{x_j}, and by N_2 a bound for $| Y(z) |$ and $| Y_{z_i}(z) |$ on $| z | = 1$, and observe that the functions $z_j Y_{z_i}(z)$, are homogeneous of degree $-k$ and their mean value over the sphere $| z | = 1$ is zero (otherwise, if $f(x) \neq 0$ and $c_{x_n} = \delta_{nj}$, the second integral in (44) would diverge as ϵ tends to zero while the remaining terms and the whole expression converge). Thus if we let ϵ

tend to zero in (44) and apply Theorem 1 in [3] (see also the remark on page 306 of the same paper) to the first two terms, we see that they represent a function of x whose L^p-norm does not exceed $AN_1N_2 \| f \|_p$ where A depends only on p and k. In the case $f \in L^2$, we apply Theorem 2 to the first term. The second term is not suitable for a direct application of Theorem 2, but the convolution integrals

$$\int_{\epsilon<|x-y|\leqq 1} (x_j - y_j) Y_{x_i}(x-y) f(y)\, dy$$

can be easily estimated by taking Fourier transforms and estimating the transform of $z_j Y_{x_i}(z)$ multiplied by the characteristic function of $\epsilon < |z| \leqq 1$ using the method used in Section 3.

Since $Y_{z_i}(z)$ is homogeneous of degree $-k-1$, it is absolutely integrable over $|z| \geqq 1$, and, on account of the estimate for $b(x,y)$, one sees readily that the third and fourth terms in (44) are dominated by convolutions of $|f(y)|$ with absolutely integrable functions. Hence, it follows from a theorem of Young that they represent functions whose L^p-norms are less than or equal to $\| f \|_p$ times the L^1-norms of those integrable functions, and an easy computation yields $AN_1N_2 \| f \|_p$ as a bound for the L^p-norms of those functions, where the constant A depends on k and α. Finally, one sees readily that, as ϵ tends to zero, the last term in (44) tends to a limit whose absolute value is dominated by $AN_1N_2 |f(x)|$, where A depends only on k. Collecting results and applying Lemma 1, we obtain

$$\| (cT - Tc) f_{x_i} \|_p \leqq A_p N_1 N_2 \| f \|_p, \tag{45}$$

for every f in L_1^p, $1 < p < \infty$, where A_p depends only on p, k and α (or β). Having established (45), we can proceed to prove the inequalities (41) and (42).

Consider the representation of Hf and H^*f given in (33). Write $a_0(x)$ for $a(x)$ and T_0 for the identity operator. Then since the $a_{nm}(x)$ are dominated in absolute value by a convergent numerical series and since the T_{nm} as operators on L^p, $1 < p < \infty$, have bounded norm for each fixed p, we may write

$$H = \sum_{n\geqq 0} a_{nm} T_{nm}, \qquad H^* = \sum_{n\geqq 0} (-1)^n T_{nm} \bar{a}_{nm}, \qquad H^{\#} = \sum_{n\geqq 0} (-1)^n \bar{a}_{nm} T_{nm},$$

where the series on the right converge in the operator norm. If f is in L_1^p, then

$$\begin{aligned}(\Lambda H - H\Lambda) f &= \sum_{l=1}^{k} R_l (\sum a_{nm} T_{nm} f)_{x_l} - \sum a_{nm} T_{nm} (\sum R_l f_{x_l}) \\ &= \sum_{l,n} R_l (a_{nm})_{x_l} T_{nm} f + \sum_{l,n} (R_l a_{nm} - a_{nm} R_l)(T_{nm} f)_{x_l}\end{aligned}$$

since the $(a_{nm})_{x_l}$ are dominated by a convergent numerical series which justifies term by term differentiation of the first series above. Now we apply (45) to each of the terms of the last series, estimating N_1 each time from the second formula in (40), and use (29) obtaining readily the first inequality in (41). The second inequality in (41) follows by an argument almost identical to the preceding one. In order to prove the third inequality in (41), we write

$$(H^*-H^\#)\Lambda f=\sum_{l=1}^{k}(H^*-H^\#)(R_lf)_{x_l}$$
$$=\sum_{l,n}(-1)^n(T_{nm}\bar{a}_{nm}-\bar{a}_{nm}T_{nm})(R_lf)_{x_l},$$

and again (45) combined with (40) and (4) yields the desired result.

The last inequality in (41) is readily seen to be an immediate consequence of the preceding ones.

Let now $H_1=\Sigma\, b_{nm}T_{nm}$, $H_2=\Sigma\, c_{nm}T_{nm}$, and consider the series of operators

$$\Sigma\, b_{nm}c_{\nu\mu}T_{nm}T_{\nu\mu}, \tag{46}$$

the sum being extended over all indices, and the series of their symbols

$$\begin{aligned}&\Sigma\, b_{nm}(x)c_{\nu\mu}(x)Y_{nm}(z')Y_{\nu\mu}(z')\gamma_n\gamma_\nu\\ &=(\Sigma\, b_{nm}(x)Y_{nm}(z')\gamma_n)(\Sigma\, c_{\nu\mu}(x)Y_{\nu\mu}(z')\gamma_\nu)=\sigma(H_1)\sigma(H_2)=\sigma(H_1\circ H_2).\end{aligned}\tag{47}$$

From the estimate (4) of the successive derivatives of $Y_n(z')$ and the formula (40) applied to the coefficients b_{nm} and $c_{\nu\mu}$, it follows that the first series in (47) converges uniformly as well as the series obtained from it by differentiating its terms with respect to coordinates of z any number of times. But then Theorem 3 implies that (46) converges in the operator norm and that (47) is precisely the symbol of (46), or, equivalently, that (46) is precisely $H_1\circ H_2$. On the other hand, since the functions $b_{nm}(x)$ and $c_{nm}(x)$ are dominated by convergent numerical series we have

$$H_1H_2=\Sigma\, b_{nm}T_{nm}c_{\nu\mu}T_{\nu\mu},\qquad H_1\circ H_2-H_1H_2=\Sigma\, b_{nm}(c_{\nu\mu}T_{nm}-T_{nm}c_{\nu\mu})T_{\nu\mu}.$$

Thus

$$(H_1\circ H_2-H_1H_2)\Lambda f=\Sigma\, b_{nm}(c_{\nu\mu}T_{nm}-T_{nm}c_{\nu\mu})T_{\nu\mu}(R_lf)_{x_l}$$
$$=\Sigma\, b_{nm}(c_{\nu\mu}T_{nm}-T_{nm}c_{\nu\mu})(T_{\nu\mu}R_lf)_{x_l}.$$

If we now compute the $c_{\nu\mu}$ and b_{nm} by means of (40) and apply (45) using (3) and (4) in order to estimate the kernel of T_{nm} and its first order derivatives, and bear in mind that the $T_{\nu\mu}$ are uniformly bounded in L^p and that, for each n, the number of distinct T_{nm} is of the order n^{k-2}, we obtain the

first inequality in (42). The second follows immediately from the first and the first inequality in (41). Theorem 5 is thus established.

THEOREM 6. *Let $\mathfrak{A}_p$ be the algebra of bounded operators on L^p, $1 < p < \infty$ generated by all singular integral operators H of type C_β^∞, $\beta > 1$, and their adjoints H^* (see definition 2 and Theorem 2). Then there exists a homomorphism h_p of $\mathfrak{A}_p$ onto the algebra of all functions $F(x,z)$ in C_β^∞ which are homogeneous of degree zero with respect to z, such that, for every singular integral operator H, the identities $h_p(H) = \sigma(H)$, $h_p(H^*) = \bar{\sigma}(H)$ hold. The kernel of h_p can be characterized as follows: K belongs to the kernel of h_p, or, equivalently, $h_p(K) = 0$, if and only if there exists a positive constant A depending on K such that $\| K\Lambda f \|_p \leqq A \| f \|_p$ for every $f \in L_1^p$. If $h_p(K)$ is bounded away from zero, then there exists $K' \in \mathfrak{A}_p$ with a two sided inverse, such that $h_p(K) = h_p(K')$.*

Every bounded operator on L^p which commutes with every operator in $\mathfrak{A}_p$ is a multiple of the identity operator.

The algebras $\mathfrak{A}_p$, $\mathfrak{A}_q$ corresponding to any two spaces L^p and L^q, $1 < p < q < \infty$, are isomorphic and there is a natural isomorphism ϕ between $\mathfrak{A}_p$ and $\mathfrak{A}_q$ such that $h_p = h_q \phi$.

We start with the following

LEMMA. *Let H be a singular integral operator of type C_β^∞, $\beta > 1$. Assume that for some positive constant A and every $f \in L_1^p$ the inequality $\| H\Lambda f \|_p \leqq A \| f \|_p$ holds. Then $H = 0$.*

Let $\mathfrak{B}$ be the class of functions which are symbols of singular integral operators with the property that $H\Lambda$ is bounded in the sense just described. Then $\mathfrak{B}$ is linear, and, on account of (42) and the definition 3, it is closed under multiplication by functions $F(x,z)$ in C_β^∞ which are homogeneous of degree zero with respect to z. Let u be a rotation of E_k about the point x_0. Then, if we denote $f[u(x)]$ by $f_u(x)$ and $\sigma(H)$ by $F(x,z)$, and define H_u and F_u by

$$F_u(x,z) = \sigma(H_u) = F[u(x), u(z+x_0) - x_0],$$

we have the following identities

$$\| f \|_p = \| f_u \|_p, \qquad (\Lambda f)_u = \Lambda f_u, \qquad (Hf)_u = H_u f_u.$$

Consequently, if $F(x,z) \in \mathfrak{B}$ then

$$\| H_u \Lambda f_u \|_p = \| H_u (\Lambda f)_u \|_p = \| (H\Lambda f)_u \|_p = \| H\Lambda f \|_p \leqq A \| f \|_p = A \| f_u \|_p$$

which shows that $F_u \in \mathfrak{B}$. Assume now that $F(x_0, z)$ is not identically zero in z. Then there exist finitely many rotations u_i of E_k about x_0 such that

$G(x,z) = \Sigma \mid F_{u_i}(x,z) \mid^2$ has the property that $G(x_0, z)$ does not vanish. Let now $a(x)$ be a function in C_β such that $a(x_0) \neq 0$ and vanishing outside a neighborhood of x_0 where $G(x,z)$ is bounded away from zero, and define $G_1(x,z) = a(x) G(x,z)^{-1}$, where $a(x) \neq 0$, and $G_1(x,z) = 0$ otherwise. Then $G_1 G z_1 \mid z \mid^{-1} = a(x) z_1 \mid z \mid^{-1}$, and since $F_{u_i} \in \mathcal{B}$, it follows that $a(x) z_1 \mid z \mid^{-1} \in \mathcal{B}$. Now $a(x) z_1 \mid z \mid^{-1}$ is the symbol of the operator $a(x) R_1$ and therefore, on account of (23), we have that

$$\| a(x) R_1 \Lambda f \|_p = \| i a(x) f_{x_1} \|_p \leqq A \| f \|_p$$

for every function f in $L_1{}^p$. But this is clearly impossible unless $a(x) = 0$ identically which contradicts our assumptions. Hence we must have $F(x_0, z) = 0$ for every z. Since the same argument applies to an arbitrary point x_0 we must have $F(x,z) = 0$ identically, and the only function in $\mathcal{B}$ is zero. This establishes the lemma.

Now let us revert to the proof of Theorem 6. Consider the class $\mathcal{B}$ of opeartors K in $\mathfrak{A}_p$ with the property that there exists a singular integral operator H and a constant A such that $\| (K - H) \Lambda f \|_p \leqq A \| f \|_p$ for every $f \in L_1{}^p$. Then $\mathcal{B}$ is clearly linear. Further, it follows from (41) and (42) that $\mathcal{B}$ is closed under multiplication. Now every singular integral operator belongs to $\mathcal{B}$, and the third inequality in (41) implies that their adjoints also belong to $\mathcal{B}$, that is, $\mathcal{B}$ is an algebra containing all singular integral operators and their adjoints. Hence $\mathcal{B}$ coincides with $\mathfrak{A}_p$.

The singular integral operator H associated with K in the manner described above is unique, as follows immediately from the preceding lemma. Now we define $h_p(K)$ to be $\sigma(H)$. Then h_p is clearly linear and, on account of (41) and (42), multiplicative. Since the mapping $H \rightarrow \sigma(H)$ is onto the class of all functions $F(x,z)$ in $C_\beta{}^\infty$ which are homogeneous of degree zero with respect to z, the same applies to h_p. The identity $h_p(H) = \sigma(H)$ for every singular integral operator H is clear, and $h(H^*) = \bar{\sigma}(H)$ follows from the third inequality in (41). Further, the fact that $h_p(K) = 0$ if and only if $K\Lambda$ is bounded in the sense described above is an immediate consequence of the definition of h_p.

Suppose now that $h_p(K) = F(x,z)$ is bounded away from zero. Let $z_0 \neq 0$ be a fixed point in E_k and set

$$a(x) = F(x, z_0) F(0, z_0)^{-1}, \qquad G(x,z) = F(x,z) a(x)^{-1} F(0,z)^{-1}.$$

Then $G(0,z) = G(x, z_0) = 1$ and this, as is readily verified, implies that $G(x,z)$ has an n-th root $G(x,z)^{1/n}$ in $C_\beta{}^\infty$. If we choose $G(x,z)^{1/n}$ so that $G(0,z)^{1/n} = 1$, the boundedness of the first order derivatives of $G(x,z)$ and the fact that $G(x, z_0) = 1$ imply that $G(x,z)^{1/n}$ converges uniformly to 1

and its derivatives with respect to coordinates of z of order $2k$ converge uniformly to zero in $|z| \geqq 1$. Thus theorem (3) implies that, for n sufficiently large, the operator H defined by $\sigma(H) = G(x,z)^{1/n}$ is close to the identity operator, or, more precisely, $\| I - H \| < \frac{1}{2}$, where I is the identity and the norm is taken in the sense of operator norm. But this implies that H has a two sided inverse. Further, define H_1 and H_2 by $\sigma(H_2) = F(0,z)$ and $\sigma(H_1) = a(x)$. Then since $a(x)$ is bounded away from zero, H_1 has an inverse, and since $F(0,z)$ does not vanish, according to the Corollary to Theorem 4, H_2 also has an inverse. Define now $K' = H_1 H_2 H^n$. Then K' has an inverse and

$$\begin{aligned} h_p(K') &= h_p(H_1) h_p(H_2) h_p(H)^n \\ &= \sigma(H_1)\sigma(H_2)\sigma(H)^n = a(x)F(0,z)G(x,z) = F(x,z) = h_p(K) \end{aligned}$$

which establishes the corresponding statement in the Lemma.

Let now K be a bounded operator on L^p which commutes with all singular integral operators. In particular, K commutes with multiplication by functions in C_β, that is, if $a(x) \in C_\beta$ then $K(af) = aK(f)$ for every $f \in L^p$. Assume now that f is positive, continuous and in L^p and consider the function $\psi(x) = f^{-1}K(f)$. Then for every $g(x)$ of the form $g(x) = f(x)a(x)$ with $a(x) \in C_\beta$ we have $K(g) = K(af) = aK(f) = af[f^{-1}K(f)] = g(x)\psi(x)$. Since K is continuous on L^p and the functions of the form $a(x)f(x)$ are dense in L^p, it follows both that $\psi(x)$ is essentially bounded and that $K(g) = \psi g$ for every $g \in L^p$. Let now $\bar{x}$ be a point at which $\psi(x)$ is equal to the derivative of its indefinite integral and $f_n(x)$ a function which is constant on the sphere with center at $\bar{x}$ and radius $1/n$, vanishes outside this sphere and has integral equal to 1. If H is a singular integral operator with kernel $h(x-y)$, then

$$HKf_n = \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} h(x-y)\psi(y)f_n(y)\,dy$$

converges towards $h(x-\bar{x})\psi(\bar{x})$ for all x, $x \neq \bar{x}$. On the other hand,

$$KHf_n = \psi(x) \lim_{\epsilon \to 0} \int_{|x-y|>\epsilon} h(x-y)f_n(y)\,dy$$

converges towards $h(x-\bar{x})\psi(x)$. Since H and K commute we have $KHf_n = HKf_n$, and therefore $h(x-\bar{x})\psi(x) = h(x-\bar{x})\psi(\bar{x})$ almost everywhere. If we assume, as we may, that $h(x)$ does not vanish identically on a set of positive measure, it follows that $\psi(x) = \psi(\bar{x})$ almost everywhere, and this implies that K is a multiple of the identity.

In order to prove the last part of the theorem, we observe that the

singular integral operators and their adjoints are defined in all spaces L^p, $1 < p < \infty$, and continuous in the corresponding topologies. Therefore an operator K in $\mathfrak{A}_p$ will map $L^p \cap L^q$ into itself, and since $L^p \cap L^q$ is dense in L^q, the restriction of K to $L^p \cap L^q$ will have a unique continuous extension to L^q, which we take as the definition of $\phi(K)$. Then one verifies that ϕ is the desired isomorphism between $\mathfrak{A}_p$ and $\mathfrak{A}_q$.

Theorem 6 is thus established.

THEOREM 7. *Let $\alpha = (\alpha_1, \cdots, \alpha_k)$ be a k-tuple of non-negative integers and write $D_\alpha u = \partial^{\alpha_1 + \cdots + \alpha_k} u / \partial x_1^{\alpha_1} \partial x_2^{\alpha_2} \cdots \partial x_k^{\alpha_k}$, $z^\alpha = z^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n}$. Let $P(u) = \sum a_\alpha(x) D_\alpha u$ be a linear partial differential operator of homogeneous order m with coefficients $a_\alpha(x)$ in C_β, $\beta \geqq 0$. Then if $u \in L_m{}^p$, $P(u) = H\Lambda^m u$ where H is a singular integral operator of type $C_\beta{}^\infty$ and*

$$\sigma(H) = (-i)^m \sum_\alpha a_\alpha(x) z^\alpha \,|\, z \,|^{-m}, \text{ where } |\, z \,| = (z_1{}^2 + \cdots + z_k{}^2)^{\frac{1}{2}}.$$

According to (23), we have $\partial u / \partial x_n = -i R_n \Lambda u$ and therefore, since the R_n and Λ commute, it follows that

$$D_\alpha u = (-i)^m R_1{}^{\alpha_1} R_2{}^{\alpha_2} \cdots R_k{}^{\alpha_k} \Lambda^m u = (-i)^m R^\alpha \Lambda^m u$$

and

$$P(u) = \sum_\alpha a_\alpha(x) D_\alpha u = (-i)^m \sum a_\alpha(x) R^\alpha \Lambda^m u.$$

Now according to (14) and (37), $\sigma(R_n) = z_n \,|\, z \,|^{-1}$ and from this the desired expression for

$$\sigma(H) = \sigma[(-i)^m \sum_\alpha a_\alpha(x) R^\alpha]$$

follows. This proves the theorem.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
CORNELL UNIVERSITY,
UNIVERSITY OF CHICAGO.

REFERENCES.

[1] H. Bateman, *Higher transcendental functions*, vol. 2, N. Y., 1953.

[2] S. Bochner, "Theta relations with spherical harmonics," *Proceedings of the National Academy of Sciences*, vol. 37 (1951), pp. 804-808.

[3] A. P. Calderón and A. Zygmund, "On singular integrals," *American Journal of Mathematics*, vol. 78 (1956), pp. 289-309.

[4] E. Heine, *Handbuch der Kugelfunktionen*, vols. I and II, 2d. ed., Berlin, 1878-1888.

[5] G. N. Watson, *A treatise on the theory of Bessel functions*, Cambridge University Press, 1922.

ON SIMPLE GROUPS OF TYPE B_n.*

By JEAN DIEUDONNÉ.

1. C. Chevalley [1] has recently defined simple linear groups over an arbitrary field K, corresponding to the classes of simple Lie algebras over the complex field; and, with one exception, R. Ree [4] has identified the groups corresponding to the classes A_n, B_n, C_n, D_n and G_2 to well-known classical groups. The exception concerns the class B_n when $n \geqq 2$ and K is an imperfect field of characteristic 2; I will prove in this note, using Ree's other results and the general structure of orthogonal groups corresponding to defective quadratic forms [2, pp. 52-60], that in that exceptional case the Chevalley group is again isomorphic to *the commutator subgroup of the orthogonal group defined by the quadratic form* $Q(x) = \sum_{i=0}^{n} \xi_i \xi_{-i}$ (with respect to a suitable basis $(e_i)_{-n \leq i \leq n}$ of a $(2n+1)$-dimensional space E over K).

2. It is proved in [4, p. 398] that the Chevalley group of type B_n leaves invariant the $2n$-dimensional subspace E_1 of E generated by the e_i of index $\neq 0$, and is isomorphic to its restriction H to that subspace. Moreover, H is generated by the matrices

$$V_{i,t} = I + t^2 E_{-ii} \text{ and } W_{i,j,t} = I + t(E_{i,-j} - E_{j,-i}),$$

where $t \in K$, and i, j take the values $\pm 1, \pm 2, \cdots, \pm n$, the E_{ij} being as usual the matrices such that $E_{ij} \cdot e_j = e_i$, $E_{ij} \cdot e_k = 0$ for $k \neq j$. Now, in the case we are considering, the K^2-subspace $\mathfrak{M}$ of K from the general theory of defective forms [2, p. 52] is reduced to K^2; therefore, for fixed i, the $V_{i,t}$ constitute *all singular orthogonal transvections* [2, p. 55] corresponding to the vector e_{-i}. But, for fixed i, the $V_{i,t}$ and $V_{-i,t}$ obviously generate the unimodular group $SL_2(K^2)$ corresponding to the K^2-plane P_i generated by e_i and e_{-i}; there is therefore in that group a matrix U which transforms e_{-i} into a vector $a \in P_i$ such that $Q(a) \neq 0$; furthermore $Q(a) \in K^2$, hence the transformations $UV_{i,t}U^{-1}$ constitute *all semi-singular orthogonal transvections* [2, p. 54] corresponding to the vector a.

* Received May 21, 1957.

Next we remark that, as $n \geqq 2$, the subgroup generated by the matrices $W_{i,j,t}$ contains the commutator subgroup $\Omega_{2n}(K, Q_1)$, where Q_1 is the restriction to E_1 of the quadratic form Q [4, p. 397]. But from Witt's theorem it is easy to deduce that for any vector $b \in E_1$ such that $Q(b) \in K^2$ and $Q(b) \neq 0$, there is a transformation of $\Omega_{2n}(K, Q_1)$ transforming a into a scalar multiple of b, and that for any vector $c \in E_1$ such that $Q(c) = 0$, there is a transformation of $\Omega_{2n}(K, Q_1)$ sending e_{-i} into a scalar multiple of c [3, § 10, 7), p. 65]. It follows that the group H contains *all* semi-singular transvections, and therefore the commutator subgroup $\Omega_{2n+1}(K, Q)$ ([2], p. 59 and [3], § 11, p. 69); on the other hand, as $W_{i,j,t}$ belongs to the orthogonal group $O_{2n}(K, Q_1)$, and a fortiori to the orthogonal group $O_{2n+1}(K, Q)$, the group $\Omega_{2n+1}(K, Q)$ is a normal subgroup of H, and is not contained in the center of H; hence $H = \Omega_{2n+1}(K, Q)$.

It may be remarked that the theorem still holds when $n = 1$. Indeed, we have seen above that H is then the unimodular group $SL_2(K^2)$, hence H contains all semi-singular transvections corresponding to vectors $\xi_1 e_1 + \xi_{-1} e_{-1}$ such that $\xi_1 \xi_{-1} \in K^2$, and these are in fact all semi-singular transvections; the argument is then concluded as above.

NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] C. Chevalley, "Sur certains groupes simples," *Tôhoku Math. J.*, (2), vol. 7 (1955), pp. 14-66.

[2] J. Dieudonné, "Sur les groupes classiques," *Actual. Scient. et Ind.*, no. 1040, Paris (Hermann), 1948.

[3] ———, *La géométrie des groupes classiques*, Erg. der Math., Neue Folge, Heft 5, Berlin (Springer), 1955.

[4] R. Ree, "On some simple groups defined by C. Chevalley," *Trans. Amer. Math. Soc.*, vol. 84 (1957), pp. 392-400.

EXTENSIONS OF REPRESENTATIONS OF LIE GROUPS AND LIE ALGEBRAS, I.*

By G. Hochschild ** and G. D. Mostow.†

1. **Introduction.** Let K be a group, G a subgroup of K, ρ a representation of G, V the representation space of ρ. We shall say that a representation σ of K is an extension of the representation ρ of G if the representation space W of σ contains V as a G-stable subspace and σ coincides with ρ in V. If we insist on remaining within the category of *finite dimensional* representations, such an extension does not always exist. In the case where G is normal in K and there is a complementary subgroup H in K such that K is a semidirect product $H \cdot G$, the extension problem for finite dimensional representations can be analyzed in terms of representative functions. In fact, using the representative functions associated with the given representation ρ of V, we shall give a standard construction yielding a representation space W for K such that W contains V as a G-stable subspace, *and is finite dimensional whenever such a representation space exists at all.* If K is a connected Lie group, and for the category of finite dimensional continuous representations, this gives a complete solution of the extendibility problem (Theorem 3.1). Moreover, we give a construction that enables us to treat the more general case where $K = HG$, with $H \cap G$ compact (Theorem 3.2).

In Section 4, we shall show how some of the basic result on the existence of faithful representations for connected Lie groups can be proved comparatively simply by means of the extension theorem. In particular, the use of Ado's theorem on the existence of a faithful representation for a Lie algebra is completely eliminated.

On the other hand, the extension theorem for representations has an analogue for Lie algebras, which is due to Zassenhaus and was used by him in proving Ado's theorem. The technique of representative functions, here defined as functions on the universal enveloping algebra, gives a very simple

* Received May 15, 1957.

** John Simon Guggenheim Fellow.

† Supported in part by a research contract with the U. S. Airforce.

and natural proof of Zassenhaus's extension theorem, and thus of Ado's theorem. We shall give this proof in Section 5, which is quite independent of what precedes.

2. Notation and general facts. Let F be a field, and let V be a vector space of finite dimension d over F. A representation ρ of a group G in V, or with representation space V, is a homomorphism of G into the group of all linear automorphisms of V. If $x \in G$ and $v \in V$, we abbreviate $\rho(x)(v)$ by $x \cdot v$. Let $E(V)$ denote the algebra of all linear endomorphisms of V. If λ is any linear map of $E(V)$ into F, the composite function $\lambda \circ \rho$ from G to F is called a *representative function* on G associated with the representation ρ. These functions make up a finite dimensional vector space $R(\rho)$ over F. If f is any function on G, and $x \in G$, we define the left translate $x \cdot f$ as the function on G that is given by $(x \cdot f)(y) = f(yx)$, for all $y \in G$. Similarly, the right translate $f \cdot x$ is defined by $(f \cdot x)(y) = f(xy)$. In particular, if $f \in R(\rho)$, then $x \cdot f$ and $f \cdot x$ belong to $R(\rho)$, for every $x \in G$. Using only the left translations, we thus have a natural representation of G in $R(\rho)$.

Let μ be any linear map of V into F, and let $v \in V$. Then we define a function $\mu/v \in R(\rho)$ by setting $(\mu/v)(y) = \mu(y \cdot v)$. Observe that $x \cdot (\mu/v) = \mu/x \cdot v$. Now let $\mu_1, \cdots, \mu_d$ be a basis for the dual space $\mathrm{Hom}_F(V, F)$ of V. Let $d \cdot R(\rho)$ stand for the direct sum of d copies of $R(\rho)$, regarded as a representation space for G in the natural fashion. We define a map of V into $d \cdot R(\rho) : v \rightarrow (\mu_1/v, \cdots, \mu_d/v)$. It is immediately verified that this is a G-monomorphism.

Let $V = V_0 \supset \cdots \supset V_n = (0)$ be a composition series for the representation space V. Let V' be the direct sum of the factor representation spaces V_i/V_{i+1}, where i ranges from 0 to $n-1$. Then V' is a semisimple representation space for G. Moreover, to within G-isomorphisms, V' is independent of the particular choice of the composition series. Hence the representation ρ' of G in V' is essentially determined by ρ; we shall call it the *semisimple representation associated with* ρ. Clearly, if ρ is a semisimple representation, ρ' may be identified with ρ.

We shall say that a representation ρ of G is *unipotent* if the representation space V has a descending series of G-stable subspaces such that the representation in each factor space of the series is trivial. It amounts to the same thing to say that ρ' is trivial. More precisely, let K be a subgroup of G. Then, if ρ' is trivial on K, it clearly follows that ρ is unipotent on K. Conversely, *if K is normal in* G, and if ρ is unipotent on K, then

ρ' is trivial on K, because every semisimple representation space for G is then semisimple as a representation space for K.

Let 1 stand for the identity transformation on V, and let K be an arbitrary subgroup of G. It is easily seen that the representation ρ of G is unipotent on K if and only if there is a positive integer n such that, for every n-tuple $x_1, \cdots, x_n$ of elements of K,

$$(1 - \rho(x_1)) \cdots (1 - \rho(x_n)) = 0.$$

It is clear from this that, if ρ is unipotent on K, so is the representation of K in $R(\rho)$, since $\Pi(1 - x_i) \cdot (\mu/v) = \mu/(\Pi(1 - \rho(x_i))(v)$. It is equally evident that a subrepresentation or a factor representation of a unipotent representation is unipotent. Similarly, a sum of unipotent representations is unipotent. Finally, the tensor product of two unipotent representations ρ and σ is unipotent, as is seen from the relation

$$1 \otimes 1 - \rho(x) \otimes \sigma(x) = (1 - \rho(x)) \otimes 1 + \rho(x) \otimes (1 - \sigma(x)).$$

It has been shown by Kolchin that ρ is unipotent if, for every $x \in G$, the transformation $1 - \rho(x)$ is nilpotent. We remark that this follows readily from Wedderburn's theorem on simple algebras. Observe first that we may asume without loss of generality that F is algebraically closed. Next, note that if we proceed by induction on the dimension of V we reduce the problem to the case where V is a simple representation space for G. Now let A be the algebra of linear endomorphisms of V that is generated by the endomorphisms $1 - \rho(x)$, with $x \in G$. Clearly, an A-stable subspace of V is also G-stable, so that V is simple as an A-module. Hence, if $A \neq (0)$, it follows from Wedderburn's theorem that A is the algebra of all linear transformations of V. On the other hand, we see immediately that every element of A is actually a finite linear combination of elements $1 - \rho(x)$, with $x \in G$. If every such element is nilpotent it follows that every element of A has trace 0. Hence A cannot contain every linear transformation of V, and therefore must be (0).

3. Extensions of representations. Let G be a Lie group. By a representation of G we shall mean a continuous representation by linear transformations of a finite dimensional vector space over the field of the real numbers. The radical of G is defined as the unique maximum solvable normal analytic subgroup of G. It is closed in G, and its Lie algebra is the radical (maximum solvable ideal) of the Lie algebra of G.

LEMMA 3.1. *Let G be a connected Lie group, R the radical of G, S a*

maximal semisimple analytic subgroup of G. Let ρ be a representation of G, and let A be a set of analytic automorphisms a of G such that (1): *for every $x \in R$, $\rho'(a(x)x^{-1}) = 1$, and* (2): *for every $x \in S$, $\rho(a(x)x^{-1}) = 1$. Then, if f is any representative function associated with ρ, the space spanned by the functions $f \circ a$, with $a \in A$, is finite dimensional.*

Proof. First we show that we may assume G to be simply connected. Let G^+ be the simply connected covering group of G, and let $p: G^+ \to G$ be the covering epimorphism. Then $f \circ p$ is a representative function on G^+ that is associated with the representation $\rho \circ p$ of G^+. The map $f \to f \circ p$ is evidently a linear monomorphism of the space of functions on G into that of G^+. Hence it suffices to show that the space spanned by the functions $f \circ a \circ p$, with $a \in A$, is finite dimensional. Now, for every $a \in A$, there is one and only one analytic automorphism a^+ of G^+ such that $p \circ a^+ = a \circ p$. We have $f \circ a \circ p = f \circ p \circ a^+$. Clearly, $\rho' \circ p$ is the semisimple representation of G^+ that is associated with the representation $\rho \circ p$ of G^+. If R^+ is the radical of G^+, then $p(R^+) = R$. For $x \in R^+$, we have $(\rho' \circ p)(a^+(x)x^{-1}) = \rho'(a(p(x))p(x)^{-1}) = 1$. Similarly, there is a maximal semisimple analytic subgroup S^+ of G^+ such that $p(S^+) = S$, and if $x \in S^+$, we have $(\rho \circ p)(a^+(x)x^{-1}) = \rho(a(p(x))p(x)^{-1}) = 1$. Hence the automorphisms a^+ satisfy the conditions of our lemma for the representation $\rho \circ p$ of G^+. Hence it suffices to prove the lemma in the case where G is simply connected, which we shall now assume.

Then G is the semidirect product $S \cdot R$. Let $\mathfrak{R}$ be the Lie algebra of R, and let $\mathfrak{T}$ be the Lie algebra of the kernel of ρ' in R. Since R is normal in G, ρ' yields a semisimple representation of R, and its differential yields a semisimple representation of $\mathfrak{R}$. Hence we may apply Lie's theorem to conclude that $[\mathfrak{R}, \mathfrak{R}] \subset \mathfrak{T}$. Let $x_1, \cdots, x_n$ be representatives in $\mathfrak{R}$ for a basis of $\mathfrak{R}/\mathfrak{T}$. Then $\mathfrak{T} \subset (\mathfrak{T}, x_1) \subset \cdots \subset (\mathfrak{T}, x_1, \cdots, x_n) = \mathfrak{R}$ is a sequence of ideals of $\mathfrak{R}$. Since R is simply connected, the analytic subgroup T of R that corresponds to the ideal $\mathfrak{T}$ of $\mathfrak{R}$ is closed in R and simply connected.[1] Since $\mathfrak{T}$ is nilpotent, the exponential map is a homeomorphism of $\mathfrak{T}$ into T.[2] Moreover, R can be reached from T by successively constructing semidirect products according to our series of ideals from $\mathfrak{T}$ to $\mathfrak{R}$. Hence we have a

[1] According to a well known result due to Malcev, every normal analytic subgroup of a simply connected Lie group is closed and simply connected. The proof is obtained by reconstructing the group through a sequence of semidirect products, as is done below for R in order to define ψ.

[2] This well known result is proved by induction on the length of the ascending central series for $\mathfrak{T}$, using the result of footnote 1.

homeomorphism ψ of $\mathfrak{R}$ onto R, where, for $u \in \mathfrak{T}$ and real numbers t_i, $\psi(u + \sum_{i=1}^{n} t_i x_i) = \exp(u)\exp(t_1 x_1) \cdots \exp(t_n x_n)$.

Every analytic automorphism $a \in A$ induces an automorphism $a\cdot$ of $\mathfrak{R}$. It follows from condition (1) that we have $a\cdot(\mathfrak{T}) \subset \mathfrak{T}$, and $a\cdot(x_i) = a_i + x_i$, with $a_i \in \mathfrak{T}$, for each i. If $z = u + \sum_{i=1}^{n} t_i x_i$, we have therefore

$$a(\psi(z)) = \exp(a\cdot(u))\exp(t_1(a_1 + x_1)) \cdots \exp(t_n(a_n + x_n)).$$

Now let $\rho\cdot$ stand for the representation of $\mathfrak{R}$ that is induved by ρ, and write $\alpha_i = \rho\cdot(a_i)$, $\zeta_i = \rho\cdot(x_i)$. Then we have

$$\rho(a(\psi(z))) = \exp(\rho a\cdot(u))\exp(t_1(\alpha_1 + \zeta_1)) \cdots \exp(t_n(\alpha_n + \zeta_n)).$$

Choose a basis $y_1, \cdots, y_q$ for $\mathfrak{T}$, and write $a\cdot(y_j) = \sum_{k=1}^{q} b_{jk} y_k$, and $a_i = \sum_{k=1}^{q} a_{ik} y_k$. Then $\alpha_i = \sum_{k=1}^{q} a_{ik}\eta_k$, where $\eta_k = \rho\cdot(y_k)$.

The representation $\rho\cdot$ is nilpotent on $\mathfrak{T}$, and $\rho\cdot(\mathfrak{T})$ is an ideal in $\rho\cdot(\mathfrak{R})$. It follows that, if d is the dimension of the representation space V of ρ, every monomial in elements of $\rho\cdot(\mathfrak{R})$ in which there occur more than $d-1$ factors in $\rho\cdot(\mathfrak{T})$ is 0.

Writing out the exponential series in our expression for $\rho(a(\psi(z)))$, we obtain the absolutely convergent series

$$\sum (\rho a\cdot(u))^{e}(\alpha_1 + \zeta_1)^{e_1} \cdots (\alpha_n + \zeta_n)^{e_n} t_1^{e_1} \cdots t_n^{e_n}(e!e_1! \cdots e_n!)^{-1},$$

where the summation goes over all $(n+1)$-tuples $(e, e_1, \cdots, e_n)$ of non-negative integers, with $e < d$. Write $u = \sum_k c_k y_k$, so that $\rho a\cdot(u) = \sum_{j,k} b_{kj} c_k \eta_j$. Now substitute this for $\rho a\cdot(u)$, and $\sum_k a_{ik}\eta_k$ for α_i, in the above, and then multiply out each term of the series in full. Each term can be written in the form $p_1 q_1(e, e_1, \cdots, e_n) + \cdots + p_r q_r(e, e_1, \cdots, e_n)$, where the p_i are the various monomials of degree $\leqq e + e_1 + \cdots + e_n$ in the coefficients b_{kj} and a_{ik} of $a\cdot$, and the $q_i(e, e_1, \cdots, e_n)$ are certain homogeneous (non-commutative) polynomials in the η_j and ζ_i whose coefficients depend on the t_i and the c_k, i.e., on z, but not on the automorphism a. It is easily seen by the usual estimate of the size of the elements of a product of matrices that, for each i, the series $\sum_{(e, e_1, \cdots, e_n)} q_i(e, e_1, \cdots, e_n)$ is absolutely convergent. Moreover, it is clear from our remark above that $q_i(e, e_1, \cdots, e_n) = 0$ whenever p_i is of degree greater than $d-1$. Hence we conclude that, if $p_1, \cdots, p_s$ are all the monomials of degree $< d$ in the coefficients of $a\cdot$, there are certain

maps $f_1, \cdots, f_s$ of $\mathfrak{R}$ into $E(V)$ (whose values are given by the sums of the series $\sum_{(e, e_1, \cdots, e_n)} q_i(e, e_1, \cdots, e_n)$) such that

$$\rho(a(\psi(z))) = p_1 f_1(z) + \cdots + p_s f_s(z).$$

Now let π denote the projection $S \cdot R \to R$, and put $g_i = f_i \circ \psi^{-1} \circ \pi$. Then, with $x \in G$, we have

$$\rho(a(\pi(x))) = p_1 g_1(x) \cdots p_s g_s(x),$$

and, using condition (2),

$$\rho(a(x)) = \rho(a(x\pi(x)^{-1}))\rho(a(\pi(x)))$$
$$= \rho(x\pi(x)^{-1})\rho(a(\pi(x))) = p_1 h_1(x) + \cdots + p_s h_s(x),$$

where $h_i(x) = \rho(x\pi(x)^{-1}) g_i(x)$. Clearly, this gives the conclusion of Lemma 3. 1.

THEOREM 3. 1. *Let K be a connected Lie group, and suppose that K is a semidirect product $H \cdot G$, with G normal in K. Let R be the radical of G, and let ρ be a representation of G such that, if ρ' is the associated semisimple representation, $\rho'(yxy^{-1}x^{-1}) = 1$, for every $y \in K$ and every $x \in R$. Then the representation space V of ρ can be G-monomorphically imbedded in a representation space W of a representation σ of K, and the kernel of σ' contains the kernel of ρ'.*

Proof. Let S be a maximal semisimple analytic subgroup of G. Let $y \in K$, and consider the automorphism of G/R that is induced by the conjugation $x \to y^{-1}xy$ of G. Since G/R is semisimple, the connected component of the identity in the group of all continuous automorphisms of G/R is the group of the inner automorphisms of G/R. Hence there is an element $u \in G$ such that the conjugation $x \to (yu)^{-1}x(yu)$ induces the identity automorphism of G/R. It follows that, for every $s \in S$, $(yu)^{-1}s(yu)s^{-1} \in R$. On the other hand, by a well known result due to Harish-Chandra,[3] any two maximal semisimple analytic subgroups of G are conjugate to each other by an inner automorphism effected by an element of R. Hence there is an element $r \in R$ such that $(yu)^{-1}S(yu) = rSr^{-1}$. Hence, for every $s \in S$, we have $(yur)^{-1}s(yur)s^{-1} \in S$. On the other hand, it follows from our first result that this element lies in R.

Now consider the continuous map $s \to (yur)^{-1}s(yur)s^{-1}$ of the analytic group S into $S \cap R$. Since $S \cap R$ is a discrete subgroup of the analytic group

[3] Cor. 3, in [4].

S, this map must be constant, whence we conclude that yur commutes with every element of S.

We extend the left G-translations of functions on G to K-operations on these functions: let f be a function on G, h an element of H, x and y elements of G. Then the function $(hx)\cdot f$ on G is defined by setting

$$((hx)\cdot f)(y) = f(h^{-1}yhx).$$

Clearly, if f is continuous, so is $(hx)\cdot f$. Furthermore, it is easily verified that $u\cdot(v\cdot f) = (uv)\cdot f$, for all u and v in K.

By what we have shown above, given any element $h \in H$, we can find an element $z \in G$ such that hz commutes with every element of S. Let a be the automorphism $x \to (hz)^{-1}x(hz)$. Then we have $h\cdot f = (z^{-1}\cdot f\cdot z)\circ a$.

Now suppose that $f \in R(\rho)$. By the assumption of our theorem, the automorphism a satisfies the conditions of Lemma 3.1. Since the functions $z^{-1}\cdot f\cdot z$ lie in the finite dimensional space $R(\rho)$, it follows therefore from Lemma 3.1 that the space spanned by the functions $h\cdot f$, as h ranges over H and f ranges over $R(\rho)$, is finite dimensional. Hence the K-transforms of the elements of $R(\rho)$ make up a finite dimensional space U of functions on G, and U is a representation space for K containing $R(\rho)$ as a G-stable subspace. We have seen in Section 2 that there is a G-monomorphism of V into $d\cdot R(\rho)$. Composing this with the injection $R(\rho) \to U$, we obtain a G-monomorphism of V into the representation space $d\cdot U$ for K. Let σ denote the representation of K in $d\cdot U$. There remains only to show that the kernel of σ' contains the kernel of ρ'.

It follows from the condition of our theorem that the kernel of ρ' is normal in K, not only in G. Indeed, let z be an element of the kernel of ρ', and let $y \in K$. We can write $z = sr$, with $s \in S$ and $r \in R$. As we have seen above, there is an element $u \in G$ such that uy commutes with every element of S. We have

$$yzy^{-1} = (ysy^{-1})(yry^{-1}) = (u^{-1}su)(yry^{-1}) = (u^{-1}zu)(u^{-1}r^{-1}u)(yry^{-1}).$$

Since the kernel of ρ' is normal in G, we have $\rho'(u^{-1}zu) = 1$. Applying ρ' to the last expression for yzy^{-1}, and using the condition of our theorem, we find therefore $\rho'(yzy^{-1}) = 1$, and we have shown that the kernel of ρ' is normal in K.

Hence it suffices to show that the representation of the kernel of ρ' in U is unipotent. The elements of U are linear combinations of function $y\cdot f$, with $y \in K$ and $f \in R(\rho)$. If z lies in the kernel of ρ', so does each conjugate $y^{-1}zy$, and we have $z\cdot(y\cdot f) = y\cdot(y^{-1}zy\cdot f)$. Since, as we have

seen in Section 2, the representation of the kernel of ρ' in $R(\rho)$ is unipotent, this shows that the representation of the kernel of ρ' in U is unipotent. This completes the proof of Theorem 3.1.

Although we shall need Theorem 3.1 only in the form stated above, we point out the following generalization.

THEOREM 3.2. *Let K be a connected Lie group, G a closed connected normal subgroup of K, ρ a representation of G satisfying the condition of Theorem 3.1. Suppose that H is an analytic subgroup of K such that $K = HG$ and $H \cap G$ is a compact subgroup of the analytic group H. Assume that there is a representation of H that is faithful on $H \cap G$. Then ρ can be extended to a representation τ of K such that the kernel of τ' contains the kernel of ρ'.*

Proof. We construct the appropriate semidirect product $H \cdot G$, so that we have the natural epimorphism $H \cdot G \rightarrow HG = K$, whose kernel consists of the elements $x \cdot x^{-1}$, with $x \in H \cap G$. Let W be the representation space for the semidirect product $H \cdot G$, as defined in the proof of Theorem 3.1. The right translations of representative functions give us the structure of a right G-module on W, because W is a direct sum of copies of a space of representative functions on G that is stable under the right translations.

Now let A denote the group algebra, over the real number field, of the group $H \cap G$. The right G-module structure of W allows us to regard W as a right A-module. Let U be a representative space for H. Then we may also regard U as a left A-module, and we can form the tensor product $W \otimes_A U$. This is the canonical homomorphic image of the tensor product $W \otimes U$ over the real number field, the kernel consisting of all finite sums of elements of the form $w \cdot x \otimes u - w \otimes x \cdot u$, where $w \in W$, $u \in U$, and $x \in H \cap G$. Clearly, $W \otimes U$ is a representation space for $H \cdot G$ such that, with $h \in H$ and $g \in G$,

$$(h \cdot g) \cdot (w \otimes u) = ((h \cdot g) \cdot w) \otimes (h \cdot u),$$

where $h \cdot g$ stands for the product of h and g in the semidirect product $H \cdot G$, not in K. It is easily verified that $(h \cdot g) \cdot (w \cdot x) = ((h \cdot g) \cdot w) \cdot hxh^{-1}$, while $h \cdot (x \cdot u) = (hxh^{-1}) \cdot (h \cdot u)$. Hence we see that the kernel of the canonical epimorphism $W \otimes U \rightarrow W \otimes_A U$ is stable under the operations with the elements of $H \cdot G$, so that we obtain the structure of a representation space for $H \cdot G$ on $W \otimes_A U$. Moreover, if $x \in H \cap G$, we have $(x \cdot x^{-1} \cdot w = w \cdot x^{-1}$, whence we see that the representation of $H \cdot G$ in $W \otimes_A U$ is trivial on the kernel of the epimorphism $H \cdot G \rightarrow K$. Thus we obtain a representation of K in $W \otimes_A U$.

Let η be a representation of H by *complex* linear automorphisms that is faithful on $H \cap G$. Since $H \cap G$ is compact, the restriction of η to $H \cap G$ and the dual representation of $H \cap G$ generate *all* representations of $H \cap G$, by the processes of forming direct sums, tensor products, and subrepresentations. This well known fact is the content of Prop. 3, p. 190, in [0]. It follows that every representation space for $H \cap G$ is an $H \cap G$—subspace of some representation space for H.

Now let J denote the set of all elements $a \in A$ such that $w \cdot a = 0$, for every $w \in W$. Then J is a two-sided ideal of A, and A/J is finite dimensional. Regard A/J as a representation space for $H \cap G$. The natural anti-monomorphism of A/J into $E(W)$ shows that the representation of $H \cap G$ in A/J is continuous. By what we have seen above, there is a representation space U for H that contains A/J as an $H \cap G$—stable subspace. As a representation space for $H \cap G$, U is semisimple, so that U is the direct sum of A/J and another $H \cap G$-stable subspace P. Thus we have the direct decomposition

$$W \otimes_A U = W \otimes_A (A/J) + W \otimes_A P,$$

and each of the two direct summands on the right is clearly a G-stable subspace of $W \otimes_A U$. Moreover, since J annihilates W from the right, the first summand is canonically isomorphic with W, as a representation space for G.

Thus, if τ is the representation of K in $W \otimes_A U$, then τ is an extension of the given representation ρ of G, via the representation of G in $W = W \otimes_A (A/J) \subset W \otimes_A U$. Furthermore, since the kernel of σ' (where σ is the representation of $H \cdot G$ in W) contains the kernel of ρ', and since, for $x \in G$, $x \cdot (w \otimes u) = (x \cdot w) \otimes u$, it follows that the kernel of τ' contains the kernel of ρ'. This completes the proof of Theorem 3.2.

Observe that *the condition imposed on* ρ *in the statement of Theorem* 3.1 *is necessary for* ρ *to be extendible to a representation of* K. Indeed, the commutators $yxy^{-1}x^{-1}$, where $y \in K$ and $x \in R$, belong to the connected component of the identity in the intersection of the commutator subgroup of G with R, on which every representation of K must be unipotent, by Lie's theorem.

Let K be a group, G a normal subgroup of K, H a subgroup of K such that $K = HG$ (not necessarily semidirect). We remark that if a representation ρ of K is unipotent on G and on H then ρ is unipotent. In showing this, let us operate with the group algebra of K. Let $h \in H$, $x \in G$. We have

$$(1-hx)=h(1-x)+(1-h), \text{ and } (1-x)h=h(1-h^{-1}xh).$$

Hence a product of such elements, $(1-h_1x_1)\cdots(1-h_qx_q)$, can be written as a sum of products of the form hu, where $h\in H$ and u is a product whose factors are either of the form $1-x$, with $x\in G$, or of the form $1-h$, with $h\in H$, the total number of factors being q. We have

$$(1-x)(1-h)=(1-x)-h(1-h^{-1}xh).$$

Hence each u can be rewritten as an integral linear combination of products of the form $h(1-h_1)\cdots(1-h_s)(1-x_1)\cdots(1-x_t)$, where h and the h_i are in H, the x_i are in G, and t is the number of factors of the form $1-x$, with $x\in G$, that occurred in the original form of u. Hence the endomorphism that corresponds to u in our representation ρ is 0 whenever t exceeds $d-1$, where d is the dimension of the representation space of ρ. On the other hand, if $t<d$ and $q\geqq d^2$, u must contain at least d *successive* factors of the form $1-h$, so that the corresponding endomorphism must again be 0. Thus the endomorphism corresponding to $(1-h_1x_1)\cdots(1-h_qx_q)$ is 0 whenever $q\geqq d^2$, which means that ρ is unipotent.

LEMMA 3.2. *In the situation of Theorem* 3.1, *suppose that G is simply connected and nilpotent, and that ρ is a unipotent representation of G. Assume also that the representation of H in the Lie algebra $\mathfrak{G}$ of G that is obtained from the adjoint representation of K is unipotent. Then the representation σ of K that is constructed in the proof of Theorem* 3.1 *is unipotent.*

Proof. The exponential map is a homeomorphism of $\mathfrak{G}$ onto G. Furthermore, if f is any element of the representation space U for K that we have constructed in the proof of Theorem 3.1, the composite map $f\circ\exp$ is a polynomial function on $\mathfrak{G}$ of degree $<d$, where d is the dimension of the representation space V of ρ; since $f\circ\exp=\lambda\circ\rho\circ\exp=\lambda\circ\exp\circ\rho^{\cdot}$, where λ is a linear function on $E(V)$. For every $h\in H$, we have

$$(h\cdot f)\circ\exp=f\circ\exp\circ(h^{-1})^{\cdot}.$$

Since the representation of H in $\mathfrak{G}$ is unipotent, so is the dual representation with operations $\mu\to\mu\circ(h^{-1})^{\cdot}$ in the space of the linear functions on $\mathfrak{G}$. The space of the polynomial functions of degree $<d$ on $\mathfrak{G}$ is a homomorphic image of a direct sum of tensor powers of the space of the linear functions on $\mathfrak{G}$, whence we see that the representation of H in this space of polynomial functions is unipotent. The map $f\to f\circ\exp$ is an H-monomorphism of U into the space of these polynomial functions, so that we may conclude that

the representation of H in U is unipotent. Hence the representation σ of K in $d \cdot U$ is unipotent on H. We know from Theorem 3.1 that σ is unipotent on G. By what we have seen above, this implies that σ is unipotent.

4. Existence of faithful representations. The results of the preceding Section greatly facilitate the proofs for the known basic results on the existence of faithful representations of connected Lie groups. We shall sketch these proofs.

THEOREM 4.1. (E. Cartan). *Let G be a simply connected solvable Lie group, and let N be the maximum nilpotent normal analytic subgroup of G. Then there exists a faithful representation of G that is unipotent on N.*

Proof. Let Z be the connected component of the identity in the center of N (actually, it is known that the center of N is connected). Then Z is closed and normal in G, and Z is simply connected. Furthermore, Z is non-trivial (unless G is trivial) so that, making an induction on the dimension of G, we may assume that there is a faithful representation of G/Z that is unipotent on N/Z. This may be regarded as a representation ρ of G that is unipotent on N and whose kernel is precisely Z. On the other hand, Z is a vector group, and we can clearly find a faithful unipotent representation of Z. We can reach N from Z by making a sequence of constructions of semidirect products each of which statisfies the requirement of Lemma 3.2. Hence, by applying Lemma 3.2 at each level, we can extend our representation of Z to a unipotent representation of N. Now we can reach G from N by making a sequence of constructions of semidirect products. Since the commutator subgroup of G lies in N, we can apply Theorem 3.1 at each level to extend our representation of N to a representation σ of G that is unipotent on N and faithful on Z. The direct sum of ρ and σ satisfies the requirements of Theorem 4.1.

For the next proofs, we need the following two facts:

1. *If a semisimple connected Lie group has a faithful representation then its center is finite.*

2. *Let G be a Lie group, and let P be a finite normal subgroup of G. Then, if G has a faithful representation, so has G/P.*

1. is well known and easy to prove.[4] As to 2., note that if G is connected, then a finite normal subgroup is necessarily in the center of G. This is the only case we need, and it is covered by a result of Goto.[5] However, it seems

[4] Lemma 5, in [2]. [5] Lemma 8, in [3].

worth while pointing out the following proof, which establishes a result that is more general than either 2. or the result of Goto.

Let ρ be the given faithful representation of G, V the representation space of ρ, L the group of all linear automorphisms of V. Let N be the normalizer of $\rho(P)$ in L. Then N is an algebraic linear group, and $\rho(P)$ is a normal subgroup of N. Moreover, since $\rho(P)$ is finite, it is an algebraic subgroup of N. By a theorem of Chevalley,[6] there is a rational representation τ of N whose kernel is exactly $\rho(P)$. The representation $\tau \circ \rho$ of G has exactly P for its kernel, and thus yields a faithful representation of G/P.

THEOREM 4.2 (Goto).[7] *Let G be a connected Lie group, and let S be a maximal semisimple analytic subgroup of G. Suppose that S has a faithful representation, and that the radical T of the commutator subgroup G' of G is closed in G, and simply connected. Then G has a faithful representation.*

Proof. Let R be the radical of G. Then R/T is a connected abelian Lie group, whence $R/T = A \times V$, the direct product of a toroidal group A and a vector group V. Let M denote the full preimage of V in R. Since T and M/T are simply connected, M is simply connected. Now $R/M = A$, and, since A is compact and M is simply connected and solvable, it follows that R is a semidirect product $B \cdot M$.[8] By Theorem 4.1, there exists a faithful representation of M that is unipotent on the maximum nilpotent normal analytic subgroup of M. Since T is contained in this maximum nilpotent normal analytic subgroup, our representation is unipotent on T. Hence we can apply Theorem 3.1 to extend our representation of M to a representation of R that is faithful on M and unipotent on T. On the other hand, since B is compact, there is a representation of R whose kernel is precisely M. Taking the direct sum of these two representations of R, we obtain a faithful representation of R that is unipotent on T.

Now let $S \cdot R$ be the semidirect product in which the multiplication is given by $(s_1, r_1)(s_2, r_2) = (s_1 s_2, s_2^{-1} r_1 s_2 r_2)$. By Theorem 3.1, our faithful representation of R can be extended to a representation of $S \cdot R$.

Now observe that the kernel of the natural epimorphism of $S \cdot R$ onto G is contained in $(S \cap R) \cdot (S \cap R)$. Since $S \cap R$ is a discrete subgroup of the analytic group S, it is contained in the center of S. Since S has a

---

[6] Prop. 11, p. 119, in [1].

[7] Essentially, Th. 10, in [3].

[8] This result is easily proved by induction from the special case where M is a vector group, which is due to Iwasawa; the generalization is given as Lemma 8.1, in [5].

faithful representation, the center of S is finite. Hence the kernel of the epimorphism $S \cdot R \to G$ is finite. By what we have said before stating Theorem 4.2, it suffices therefore to show that the semidirect product $S \cdot R$ has a faithful representation. We have already obtained a representation of $S \cdot R$ that is faithful on R. Using a faithful representation of S in addition, we obtain a faithful representation of $S \cdot R$. This completes the proof.

We remark that *the conditions of Theorem* 4.2 *are necessary for the existence of a faithful representation.*[9]

THEOREM 4.3 (Malcev).[10] *Let G be a connected Lie group, R the radical of G. Suppose that R has a faithful representation, and that one (and hence every) maximal semisimple analytic subgroup of G has a faithful representation. Then G has a faithful representation.*

Proof. By Lie's theorem, every representation of R is unipotent on the commutator subgroup R' of R. It follows that the image of R' under the representation is closed in the full linear group, and simply connected. Since R has a faithful representation, it follows that R' is closed in R, and simply connected. Hence we can proceed exactly as in the beginning of our proof of Theorem 4.2, using R' in the place of T, to show that R is a semidirect product $A \cdot M$, where A is a toroidal group and M is a simply connected normal closed subgroup of R that contains R'.

Let $\mathfrak{G}$, $\mathfrak{R}$, $\mathfrak{A}$ denote the Lie algebras of G, R, A, respectively. Since A is compact, the representation of A in $\mathfrak{G}$ that is obtained from the adjoint representation of G is semisimple. Hence $\mathfrak{G}$ is semisimple as an $\mathfrak{A}$-module, whence $\mathfrak{G}$ is the direct sum of the submodule $[\mathfrak{A}, \mathfrak{G}]$ and the centralizer $\mathfrak{P}$ of $\mathfrak{A}$ in $\mathfrak{G}$. Since $[\mathfrak{A}, \mathfrak{G}] \subset \mathfrak{R}$, we have therefore $\mathfrak{G} = \mathfrak{P} + \mathfrak{R}$. Now let $\mathfrak{S}$ be a maximal semisimple subalgebra of $\mathfrak{P}$. Clearly, $\mathfrak{S}$ is then also a maximal semisimple subalgebra of $\mathfrak{G}$. Now $\mathfrak{A} + [\mathfrak{R}, \mathfrak{R}]$ is an $\mathfrak{S}$-submodule of $\mathfrak{R}$, and $\mathfrak{A} \cap [\mathfrak{R}, \mathfrak{R}] = (0)$. Hence we can write the $\mathfrak{S}$-module $\mathfrak{R}$ as a direct sum $\mathfrak{A} + \mathfrak{B}$, where $\mathfrak{B}$ is an $\mathfrak{S}$-submodule containing $[\mathfrak{R}, \mathfrak{R}]$. Hence $\mathfrak{B}$ is an ideal of $\mathfrak{G}$, the corresponding analytic subgroup B of R is normal in G, and $R = AB$. Furthermore, our Lie algebra decomposition shows that the radical T of G' is contained in B, because the Lie algebra of T is $[\mathfrak{G}, \mathfrak{R}] = [\mathfrak{S}, \mathfrak{R}] + [\mathfrak{R}, \mathfrak{R}] = [\mathfrak{S}, \mathfrak{B}] + [\mathfrak{R}, \mathfrak{R}] \subset \mathfrak{B}$.

Now consider the natural epimorphism $B/R' \to R/(AR')$. The kernel of this epimorphism is the discrete subgroup $B/R' \cap (AR')/R'$ of the analytic group B/R'. On the other hand, the image $R/(AR')$ is isomorphic

[9] See [3]; or Th. 7.3, in [5].
[10] [6]; or Th. 7, in [3].

with M/R', which is a vector group. Hence $R/(AR')$ has no non-trivial covering, whence our epimorphism must be an isomorphism. Thus we have $B/R' \cap (AR')/R' = (1)$, and B/R' is simply connected. It is clear from the former that the natural epimorphism $(AR')/R' \times B/R' \to R/R'$ is an isomorphism. Consequently, B/R' is closed in R/R'. Hence B is closed in R, and therefore in G. In addition, B is simply connected, because both R' and B/R' are simply connected.

As a normal analytic subgroup of the simply connected group B, the radical T of G' is closed in B, and simply connected. Hence it is clear that the assumptions of Theorem 4.2 are satisfied. We conclude from Theorem 4.2 that G has a faithful representation, and our proof is complete.

It is evident that the conditions of Theorem 4.3 are necessary for the existence of a faithful representation of G.

5. Faithful representations of Lie algebras. Let L be a finite dimensional Lie algebra over a field F of characteristic 0, and let K be an ideal of L. We assume that there is a subalgebra H of L such that L is the semidirect sum $H + K$. Let $U(L)$, $U(K)$ denote the universal enveloping algebras of L, K, respectively. We define right L-operations on $U(K)$ as follows: let $u \in U(K)$, $h \in H$, $k \in K$. We define $u \cdot (h + k) = uh - hu + uk$, observing that, since K is an ideal of L, $uh - hu$ lies in $U(K)$, where we regard $U(K)$ as a subalgebra of $U(L)$ in the natural fashion. It can be verified immediately that, for arbitrary elements x and y of L, we have

$$(u \cdot x) \cdot y - (u \cdot y) \cdot x = u \cdot [x, y].$$

It follows that these right L-operators on $U(K)$ define the structure of a right $U(L)$-module on $U(K)$. We make the dual space $\mathrm{Hom}_F(U(K), F)$ into a left $U(L)$-module accordingly: $(x \cdot f)(u) = f(u \cdot x)$.

A representation ρ of K gives rise in the canonical fashion to a representation, which we still denote by ρ, of the associative algebra $U(K)$. If V is the representation space of ρ, and λ is any linear map of $E(V)$ into F, then the composite function $\lambda \circ \rho$ on $U(K)$ is called a *representative function* associated with ρ. As before, we shall always assume that V is finite dimensional.

The kernel of ρ in $U(K)$ is a two sided ideal I of $U(K)$. Since V is finite dimensional, $U(K)/I$ is finite dimensional, i.e., I is of finite codimension in $U(K)$. The representative functions associated with ρ vanish on I, and constitute a finite dimensional space $R(\rho)$ over F. Clearly, $R(\rho)$ is a $U(K)$-submodule (though not always a $U(L)$-submodule) of $\mathrm{Hom}_F(U(K), F)$.

$U(K)$ has a natural increasing filtration by the subspaces $U(K)_m$ $(m=0,1,\cdots)$ consisting of the elements that can be written as (non-commutative) polynomials of degree $\leqq m$ in the elements of K $(U(K)_0 = F)$. The associated graded algebra $\sum_m U(K)_m/U(K)_{m-1}$ is isomorphic with the symmetric algebra built over K, i.e., with a polynomial algebra in n variables, where n is the dimension of K. One verifies easily from this that $U(K)$ satisfies the maximal condition for ideals. On the other hand, one shows easily that, if A is any algebra, and I and J are ideals of finite codimension in A one of which is finitely generated as an A-module, then the product ideal IJ is of finite codimension in $U(K)$. Hence the important fact (first proved and utilized by Zassenhaus) that *the product of ideals of finite codimension in $U(K)$ is of finite codimension.*

In these terms, we can give a simple proof for the following extension theorem.

THEOREM 5.1 (Zassenhaus).[11] *Let L be a finite dimensional Lie algebra over a field F of characteristic 0, let K be an ideal of L, and suppose that L is a semidirect sum $H+K$, where H is a subalgebra. Let ρ be a finite dimensional representation of K, and suppose that $\rho'([H,K])=(0)$, where ρ' is the semisimple representation associated with ρ. Then the representation space V of ρ can be K-monomorphically imbedded in a finite dimensional representation space W for L. If σ is the representation of L in W the kernel of σ' contains the kernel of ρ'. Furthermore, if H is nilpotent on K, under the adjoint representation, then $\sigma'(H)=(0)$.*

Proof. Let I, I' be the kernels of ρ, ρ', respectively, in $U(K)$. Then it is clear that $(I')^d \subset I$, where d is the dimension of V. Since $[H,K]\subset I'$, it follows that $uh-hu \in I'$, for every $u\in U(K)$ and every $h\in H$. Hence $(I')^d$ is a $U(L)$-submodule of $U(K)$. Hence, for every $f\in R(\rho)$ and every $x\in U(L)$, the function $x\cdot f$ vanishes on $(I')^d$. Since, by what we have said above, $(I')^d$ is of finite codimension in $U(K)$, it follows that the $U(L)$-submodule S of $\mathrm{Hom}_F(U(K),F)$ that is generated by $R(\rho)$ is finite dimensional and is annihiliated by $(I')^d$.

Now (cf. § 2) we have a $U(K)$-monomorphism $V\to d\cdot R(\rho)$. Composing this with the injection $R(\rho)\to S$, we obtain a $U(K)$-monomorphism $V\to d\cdot S = W$. Since $(I')^d$ annihilates S, our representation σ of L in W is nilpotent on the ideal $I'\cap K$ of L. Hence, using that, for any ideal P of L, and any L-module M, $P\cdot M$ is an L-submodule of M, we conclude that the

[11] See [7], which also establishes the required facts concerning the universal enveloping algebra.

associated semisimple representation σ' annihilates $I' \cap K$, i.e., the kernel of σ' contains the kernel of ρ'.

Now suppose that H is nilpotent on K. Then, for every $u \in U(K)$, there is an integer n such that $u \cdot (h_1 \cdots h_n) = 0$, for all $h_i \in H$. Since $U(K)/(I')^d$ is finite dimensional, this shows that the (anti-)representation of H in $U(K)/(I)^d$ is nilpotent, whence the representation of H in S is nilpotent. Thus our representation σ is nilpotent on the ideal $I' \cap K$ and on the subalgebra H. By an elementary combinatorial argument (easier than the group analogue of § 3), it follows that σ is nilpotent on $H + I' \cap K$. Since this is an ideal of L, it must therefore be contained in the kernel of σ'. This completes the proof of Theorem 5. 1.

The existence of a faithful representation for a finite dimensional Lie algebra L over a field F of characteristic 0 is easily deduced from Theorem 5. 1. Let N be the maximum nilpotent ideal of L, R the radical of L, S a maximal semisimple subalgebra of L. We shall prove that *there is a faithful representation of L that is nilpotent on N.*

Let Z be the center of L. The adjoint representation of L is nilpotent on N and has kernel Z. There is a chain $N = N_0 \supset \cdots \supset N_r = Z$ of ideals of N such that each N_i/N_{i+1} is 1-dimensional, so that N_i is a semidirect sum of N_{i+1} and the 1-dimensional Lie algebra. Starting with a faithful nilpotent representation of Z, we apply Theorem 5. 1 repeatedly to construct a nilpotent representation of N that is faithful on Z.

Now there is a chain $R = R_0 \supset \cdots \supset R_q = N$ of ideals of R such that each R_j/R_{j+1} is 1-dimensional. Using only the first part of Theorem 5. 1, noting that $[R, R] \subset N$, we extend our representation of N to a representation of R that is still nilpotent on N and faithful on Z.

Finally, since L is the semidirect sum $S + R$ and $[S, R] \subset N$, we can extend our representation of R to a representation of L that is nilpotent on N and faithful on Z. The direct sum of this representation and the adjoint representation satisfies our requirements.

6. Correspondence between representative functions. Let G be a connected Lie group, let $\mathfrak{G}$ be the Lie algebra of G, and let $U(\mathfrak{G})$ be the universal enveloping algebra of $\mathfrak{G}$. Let A be the algebra of all real analytic functions on G. The elements of $\mathfrak{G}$ are left invariant infinitesimal transformations on G, in the sense of § II, Ch. IV of [0]. Hence A has the structure of a $\mathfrak{G}$-module, the elements of $\mathfrak{G}$ acting as derivations on A that commute with the right translations. Accordingly, we may regard A as a left $U(\mathfrak{G})$-module.

For an element u of $\mathfrak{G}$, we denote by e_u the corresponding homomorphism of the additive group R of the real line into G, i.e., $e_u(r) = \exp(ru)$, for every real number r. Let $f \in A$, $x \in G$, and put $g(r) = (x \exp(ru))$. Then g is a real analytic function on R, and it follows from the definition of the exponential map exp that the n-th derivative $g^{(n)}$ of g is equal to $(u^n \cdot (f \cdot x)) \circ e_u$ where u^n is the n-th power of u in $U(\mathfrak{G})$. Since the $U(\mathfrak{G})$-operations on A commute with the right translations, we have $g^{(n)} = ((u^n \cdot f) \cdot x) \circ e_u$. Hence, for all r in a sufficiently small neighborhood of 0 in R,

$$f(x \exp(ru)) = \sum_{n=0}^{\infty} (u^n \cdot f)(x) \cdot r^n/n!$$

Now, for every $f \in A$, let us define the function $f^{\cdot}$ on $U(\mathfrak{G})$ by setting $f^{\cdot}(u) = (u \cdot f)(1)$, for every $u \in U(\mathfrak{G})$, where 1 denotes the identity element of G. Clearly, the map $f \rightarrow f^{\cdot}$ is a linear map of A into the dual space $\mathrm{Hom}_R(U(\mathfrak{G}), R)$ of $U(\mathfrak{G})$. Moreover, if $f^{\cdot} = 0$, we conclude from the above that, for every $u \in \mathfrak{G}$, $f \circ e_u$ vanishes on some neighborhood of 0 in R, whence we conclude that f vanishes on some neighborhood of 1 in G. Since f is analytic everywhere on G, and since G is connected, this implies that $f = 0$. Thus our map $f \rightarrow f^{\cdot}$ is a linear monomorphism.

Now let ρ be a representation of G, and let V be the representation space of ρ. Let $f = \lambda \circ \rho$ be a representative function on G that is associated with ρ, i.e., λ is a linear function on $E(V)$. Let $\rho^{\cdot}$ be the representation of $U(\mathfrak{G})$ in V that is induced by ρ. We claim that $(\lambda \circ \rho)^{\cdot} = \lambda \circ \rho^{\cdot}$. The proof is as follows.

Let $x \in G$, $u \in \mathfrak{G}$. We have

$$(u \cdot (\lambda \circ \rho))(x) = ((u \cdot (\lambda \circ \rho)) \cdot x)(1) = (u \cdot ((\lambda \circ \rho) \cdot x))(1) = (u \cdot ((\lambda \cdot \rho(x)) \circ \rho))(1),$$

where $\lambda \cdot \rho(x)$ is the linear function on $E(V)$ that is defined by $(\lambda \cdot \rho(x))(e) = \lambda(\rho(x)e)$. By the above, with r in a neighborhood of 0 in R,

$$((\lambda \cdot \rho(x)) \circ \rho)(\exp(ru)) = \sum_{n=0}^{\infty} (u^n \cdot ((\lambda \cdot \rho(x)) \circ \rho))(1) \cdot r^n/n!.$$

The expression on the left can be written $\lambda(\rho(x) \exp(r\rho^{\cdot}(u)))$. If we expand this in a power series in r, and then compare the coefficients of r on the two sides above, we find that

$$\lambda(\rho(x)\rho^{\cdot}(u)) = (u \cdot (\lambda \cdot \rho(x)) \circ \rho))(1).$$

Hence we see from the first result of this proof that $u \cdot (\lambda \circ \rho) = (\rho^{\cdot}(u) \cdot \lambda) \circ \rho$, where $(\rho^{\cdot}(u) \cdot \lambda)(e) = \lambda(e\rho^{\cdot}(u))$. Clearly, this last result generalizes imme-

diately to arbitrary elements u of $U(\mathfrak{G})$. Evaluating these functions at 1, we obtain $(\lambda\circ\rho)\cdot(u)=\lambda(\rho\cdot(u))$, which is the result to be proved.

Let W be a finite dimensional space consisting of representative functions on G, and suppose that W is stable under the left translations, so that W is a representation space for G. Let τ denote the representation of G in W, and let $\tau\cdot$ be the induced representation of $U(\mathfrak{G})$ in W. If $u\in\mathfrak{G}$, and r is any real number, the left translation on W that is effected by the element $\exp(ru)$ of G is then given by $\exp(r\tau\cdot(u))$. Thus we have, for every $x\in G$ and every $f\in W$,

$$f(x\exp(ru))=\sum_{n=0}^{\infty}(\tau\cdot(u))^n(f)(x)\cdot r^n/n!.$$

Comparing this with our general result (for r in some neighborhood of 0 in R) we find that $\tau\cdot(u)(f)=u\cdot f$, for every $f\in W$ and every $u\in\mathfrak{G}$. This generalizes immediately to arbitrary elements $u\in U(\mathfrak{G})$. Thus W is a $U(\mathfrak{G})$-stable subspace of A, and the $U(\mathfrak{G})$-module structure of W that is induced by that of A coincides with the $U(\mathfrak{G})$-module structure given by $\tau\cdot$. In particular, it follows immediately from this that the image $W\cdot$ of W under the map $f\to f\cdot$ is a $U(\mathfrak{G})$-submodule of $\mathrm{Hom}_R(U(\mathfrak{G}),R)$, for the module structure we have defined at the beginning of Section 5, and that this $U(\mathfrak{G})$-module structure of $W\cdot$ coincides with the structure that is obtained by transporting $\tau\cdot$ to $W\cdot$ through the isomorphism $f\to f\cdot$.

Now let us consider a semidirect product $H\cdot G$ and a representation ρ of G, as in Theorem 3.1. We have $R(\rho)\cdot=R(\rho\cdot)$, by the above. In the proof of Theorem 3.1 we have obtained a representation space U for $H\cdot G$. U is the space of representative functions on G that is spanned by the transforms $h(f)$, with $h\in H$ and $f\in R(\rho)$, where $h(f)(x)=f(h^{-1}xh)$. Let a_h denote the conjugation with h in G, i.e., $a_h(x)=hxh^{-1}$. Then $h(f)=f\circ(a_h)^{-1}$. Let $h\cdot$ denote the automorphism of $\mathfrak{G}$ that is induced by a_h. Then we have, with $u\in\mathfrak{G}$,

$$u\cdot(h(f))=u\cdot(f\circ(a_h)^{-1})=((h^{-1})\cdot(u)\cdot f)\circ(a_h)^{-1}=h((h^{-1})\cdot(u)\cdot f).$$

Passing to the induced Lie algebra representation of the Lie algebra $\mathfrak{H}$ of H, we deduce that, with $v\in\mathfrak{H}$,

$$u\cdot(v(f))=v(u\cdot f)+[u,v]\cdot f.$$

This generalizes immediately to arbitrary elements $u\in U(\mathfrak{G})$, where $[u,v]=uv-vu$. Since, for every $f\in U$, $h(f)(1)=f(1)$, for every $h\in H$, we have $v(f)(1)=0$, for every $v\in\mathfrak{H}$. Hence, evaluating the above at 1, we find that $(v(f))\cdot(u)=f\cdot([u,v])$.

Thus our isomorphism $f \rightarrow f^{\cdot}$ transports the $\mathfrak{H}$-operations on U to the $\mathfrak{H}$-operations we have defined at the beginning of Section 5. Since U is the $\mathfrak{H}$-module generated by $R(\rho)$, it follows that $U^{\cdot}$ is the $\mathfrak{H}$-module generated by $R(\rho)^{\cdot} = R(\rho^{\cdot})$. Moreover, we can conclude from what we have seen above that, if σ is the representation of $H \cdot G$ in U, the isomorphism $U \rightarrow U^{\cdot}$ transports the representation $\sigma^{\cdot}$ of the Lie algebra $\mathfrak{H} + \mathfrak{G}$ of $H \cdot G$ to the representation of $\mathfrak{H} + \mathfrak{G}$ in $U^{\cdot}$ that we have used in the proof of Theorem 5.1. Thus *the representation of* $\mathfrak{H} + \mathfrak{G}$ *that is obtained in Theorem* 5.1 *may be identified with the differential of the representation of* $H \cdot G$ *that is obtained in Theorem* 3.1.

We can therefore apply Theorem 5.1 to conclude that, *if the representation of* H *in* $\mathfrak{G}$ *that is obtained from the adjoint representation of* $H \cdot G$ *is unipotent, then* H *is contained in the kernel of the representation* σ' *of Theorem* 3.1.

INSTITUTE FOR ADVANCED STUDY.

REFERENCES.

[0] C. Chevalley, *Theory of Lie groups*, Princeton, 1946.

[1] ———, *Théorie des groupes de Lie*, vol. III, Paris, 1955.

[2] M. Goto, "Faithful representations of Lie groups I," *Mathematicae Japonicae*, vol. 1 (1948), pp. 1-13.

[3] ———, "Faithful representations of Lie groups II," *Nagoya Mathematical Journal*, vol. 1 (1950), pp. 91-107.

[4] Harish-Chandra, "On the radical of a Lie algebra," *Proceedings of the American Mathematical Society*, vol. 1 (1950), pp. 14-17.

[5] G. Hochschild and G. D. Mostow, "Representations and representative functions of Lie groups," forthcoming in *Annals of Mathematics*.

[6] A. Malcev, "On linear groups," *Comptes rendus de l'Académie des Sciences de l'U.R.S.S.*, vol. 40 (1943), pp. 87-89.

[7] H. Zassenhaus, "Über die Darstellungen der Lie-Algebren bei Charakteristik 0," *Commentarii Mathematici Helvetici*, vol. 26 (1952), pp. 252-274.

NOTE ON CONVERGENCE OF THE PRODUCT OF BASIC SETS OF POLYNOMIALS.*

By M. Nassif.

1. In his paper [1], W. F. Newns considered my note which appeared in this Journal some time ago [2]. Newns has shown that Theorem I of [2] is false and consequently, Theorem II, which depends for its proof on Theorem I, remains unproved. In the present note a modified version of the unproved Theorem II is established. For simplicity the notations used here, apart from those newly defined, are those of Newns paper to which the reader is referred.[1] Let $\{{}^*p_n(z)\}$ be the inverse of the W-basic set $\{p_n(z)\}$ [1; p. 455, l. 17] and let $M(r) = \lim\{M_n(r)\}^{1/n}$ as $n \to \infty$, if the limit exists. The result to be established is the following theorem.

Theorem. *Let $\{p_n^{(1)}(z)\}$ be a W-basic set of polynomials and let $\{p_n^{(2)}(z)\}$ be another W-basic set for which*[2]

$$d_n^{(2)} = O(n), \qquad {}^*d_n^{(2)} = O(n), \tag{1.1}$$

as n tends to infinity. Suppose further that the set $\{p_n^{(2)}(z)\}$ is effective in $|z| \leqq R$, where

$$M^{(2)}(R) = aR, \qquad 0 < a < \infty\,; R > 0, \tag{1.2}$$

and that $\kappa^{(1)}(aR+)$ is finite. Then the product set $\{p_n(z)\}$ of the two sets $\{p_n^{(1)}(z)\}$ and $\{p_n^{(2)}(z)\}$, in the given order, will be effective in $|z| \leqq R$ if, and only if, the set $\{p_n^{(1)}(z)\}$ is effective in $|z| \leqq aR$.

In our notations, C denotes positive finite constants which are not generally of the same value at different occurrences, and ρ will be always written for aR. Now, for any set $\{p_n(z)\}$ satisfying (1.1), there exist finite numbers $\alpha > 1$, $\beta > 1$ such that

* Received March 5, 1956; revised January 20, 1957.

[1] Newns' notations used here are those defined in the following places of his paper: p. 445, l. 30; p. 446, ll. 8, 11, 23, 27-29; p. 447, l. 2; p. 455, l. 25; p. 458, ll. 7, 8 and finally p. 464, l. 16.

[2] Newns convention of notations [cf. 1; p. 456, l. 7] is adopted here also. Thus $d_n^{(2)}$ and ${}^*d_n^{(2)}$ are the degrees of the polynomials $p_n^{(2)}(z)$ and ${}^*p_n^{(2)}(z)$ respectively.

(1.3a) $\quad d_n \leqq \alpha n,\qquad$ (1.3b) $\quad {}^*d_n \leqq \beta n. \qquad (n \geqq 1)$

The proof of the above theorem depends on two lemmas.

2. LEMMA 1. *Let* $\{p_n(z)\}$ *be a W-basic set which is effective in* $|z| \leqq R$, *where*

$$M(R) = \rho. \tag{2.1}$$

If ${}^*d_n = O(n)$, *then*

$$^*M(\rho) = R. \tag{2.2}$$

If, moreover, $d_n = O(n)$ *then the inverse set* $\{{}^*p_n(z)\}$ *will be effective in* $|z| \leqq \rho$.

This lemma can be derived from Theorem 18.1 of Newns paper [cf. 1; pp. 459, 460]. For sake of completeness a direct proof is given here.

In fact, choosing a positive number $\rho_1 < \rho$ and finite numbers $\rho_2 > \rho$, $R_1 > R$ then it follows from (2.1) and the effectiveness of $\{p_n(z)\}$ in $|z| \leqq R$ that

$$\rho_1{}^n < CM_n(R) < C\rho_2{}^n \tag{2.3}$$

$$\omega_n(R) < CR_1{}^n. \qquad (n \geqq 0). \tag{2.4}$$

Hence, in view of (1.3b), (2.3) and (2.4) yield

$$^*M_n(\rho) < \sum_k |\pi_{nk}|\rho^k < C(\rho/\rho_1)^{\beta n}R_1{}^n. \tag{2.5}$$

It readily follows, in view of (1.3a), that

$$^*\omega_n(\rho) = \sum_k |p_{nk}|\,{}^*M_k(\rho) < C(\alpha n+1)(\rho/\rho_1)^{\alpha\beta n}M_n(R_1). \tag{2.6}$$

Also, applying (1.3b) and (2.3) we obtain

$$R^n \leqq \omega_n(R) = \sum_k |\pi_{nk}|\, M_k(R) < C(\beta n+1)\,{}^*M_n(\rho_2). \tag{2.7}$$

Now, from (1.3) and (2.1) it easily follows that

$$\mu(R_1)/R_1{}^\alpha \leqq \mu(R)/R^\alpha = \rho/R^\alpha;\quad {}^*\nu(\rho_2)/\rho_2{}^\beta \leqq {}^*\nu(\rho)/\rho^\beta. \tag{2.8}$$

Taking the n-th root and making n tend to infinity, (2.5), (2.7) and (2.6) respectively yield

$$^*\mu(\rho) \leqq (\rho/\rho_1)^\beta R_1;\quad R \leqq {}^*\nu(\rho_2);\quad {}^*\lambda(\rho) \leqq (\rho/\rho_1)^{\alpha\beta}\mu(R_1).$$

Hence (2.8) gives

$$^*\mu(\rho) \leqq (\rho/\rho_1)^\beta R_1; \quad R \leqq (\rho_2/\rho)^{\beta *}\nu(\rho); \quad ^*\lambda(\rho) \leqq \rho(\rho/\rho_1)^{\alpha\beta}(R_1/R)^\alpha.$$

Finally, since R_1 can be taken as near to R as we please and ρ_1 and ρ_2 are taken arbitrarily near to ρ we conlclude that

$$^*\mu(\rho) \leqq R; \quad ^*\nu(\rho) \geqq R; \quad ^*\lambda(\rho) \leqq \rho.$$

The first two relations imply (2.2) and the third implies that the inverse set $\{^*p_n(z)\}$ is effective in $|z| \leqq \rho$; and the lemma is proved.

The following examples show that, in both assertions of the lemma the condition that $^*d_n = O(n)$ cannot be dropped, while if $^*d_n = O(n)$ and $\limsup_{n\to\infty} d_n/n = \infty$, (2.2) may hold although the inverse set may not be effective in $|z| \leqq \rho$.

Example 1. Let $m_k = 2^{2^k}$, where k is a positive integer or zero, and let c be a real number greater than 1. It is easily seen that, for the set $\{p_n(z)\}$, given by

$$p_{m_k}(z) = c^{-m_k^{\frac{1}{2}}} z^{m_k}; \quad p_n(z) = c^{-n^{\frac{1}{2}}}(z^n - z^{n+1}), \quad n \neq m_k; k \geqq 0,$$

$$M(r) = r; \quad r > 0, \quad d_n = O(n), \quad \limsup_{n\to\infty} {}^*d_n/n = \infty;$$

and that the set is effective in $|z| \leqq 1$. For the inverse set $\{^*p_n(z)\}$, it can be verified that $^*\mu(1) \geqq c > 1$, and that it is not effective in $|z| \leqq 1$.

Example 2. It is easily verified that the set $\{p_n(z)\}$, given by

$$p_{m_k}(z) = c^{-m_k^{\frac{1}{2}}} z^{m_k}; \quad p_n(z) = c^{-n^{\frac{1}{2}}} \sum_{j=n}^{m_{k+1}} z^j, m_k < n < m_{k+1}; \quad k \geqq 0,$$

where m_k and c are defined in Example 1, is effective in $|z| \leqq 1$ where $M(1) = 1$. It is also seen that $^*d_n = O(n)$, while $\limsup_{n\to\infty} d_n/n = \infty$. Now the inverse set $\{^*p_n(z)\}$ can be shown to be not effective in $|z| \leqq 1$ while $^*M(1) = 1$.

3. LEMMA 2. *Let $\{p_n^{(1)}(z)\}$ be any W-basic set of polynomials and let $\{p_n^{(2)}(z)\}$ be another W-basic set satisfying* (1.1) *and* (1.2). *Then, for the product set $\{p_n(z)\}$, we have*

$$\kappa(R+) \leqq \lambda^{(2)}(R)\{\kappa^{(1)}(\rho+)/\rho\}^\beta. \tag{3.1}$$

For let ρ' be any finite number greater than ρ and choose the numbers

ρ_1 and ρ_2 such that $0 < \rho_1 < \rho < \rho_2 < \rho' < \infty$. Then choosing the number $r > R$ such that $(r/R)^a < \rho_2/\rho$, it easily follows from (1.2), (1.3) and the properties of $\mu(r)$ that $\mu^{(2)}(r) < \rho_2$; so that

$$M_n^{(2)}(r) < C\rho_2^n \qquad (n \geqq 0). \tag{3.2}$$

Also, (1.2) implies that

$$\rho_1^n < CM_n^{(2)}(R) \qquad (n \geqq 0). \tag{3.3}$$

Now choose the integers s_n and t_n for the product set $\{p_n(z)\}$, so that

$$F_n(r) = \max_{|z|=r} \left| \sum_{i=s_n}^{t_n} \pi_{ni} p_i(z) \right| = \max_{|z|=r} \left| \sum_k \pi_{nk}^{(2)} f_k(z) \right|, \tag{3.4}$$

where $f_k(z) = \sum_{i=s_n}^{t_n} \pi_{ki}^{(1)} p_i(z)$. Write $g_k(z) = \sum_{i=s_n}^{t_n} \pi_{ki}^{(1)} p_i^{(1)}(z)$, then if $g_k(z) = \sum_j g_{kj} z^j$, it follows that

$$f_k(z) = \sum_j g_{kj} p_j^{(2)}(z). \tag{3.5}$$

Let $A_k(\tau) = \max_{|z|=\tau} |f_k(z)|$; applying Cauchy's inequality to $g_k(z)$ we easily obtain from (3.2) and (3.5),

$$A_k(r) < \sum_{j=0}^{\infty} M_j^{(2)}(r) F_k^{(1)}(\rho')/\rho'^j < CS(\rho_2, \rho') F_k^{(1)}(\rho'),$$

where $S(\rho_2, \rho')$ is bounded. Inserting this in (3.4) and applying (3.3) it follows that

$$\begin{aligned} F_n(r) &< \sum_k |\pi_{nk}^{(2)}| A_k(r) < CS(\rho_2, \rho') \sum_k |\pi_{nk}^{(2)}| M_k^{(2)}(R) F_k^{(1)}(\rho')/\rho_1^k \\ &< CS(\rho_2, \rho') \omega_n^{(2)}(R) F_{\sigma_n}^{(1)}(\rho')/\rho_1^{\sigma_n}, \end{aligned} \tag{3.6}$$

where $F_{\sigma_n}^{(1)}(\rho')/\rho_1^{\sigma_n} = \max_k F_k^{(1)}(\rho')/\rho_1^k > 1$. If σ_n remains finite as n tends to infinity, (3.6) yields

$$\kappa(r) \leqq \lambda^{(2)}(R). \tag{3.7}$$

If, on the other hand, $\limsup \sigma_n = \infty$, (3.6) gives, in view of (1.3),

$$\kappa(r) \leqq \lambda^{(2)}(R) \{\kappa^{(1)}(\rho')/\rho_1\}^{\beta}. \tag{3.8}$$

Finally, since ρ' and ρ_1 can be taken arbitrarily near to ρ, and since r tends to R as ρ' tends to ρ, the required relation (3.1) follows readily from (3.7) and (3.8).

4. *Proof of the Theorem.* Suppose that the set $\{p_n^{(2)}(z)\}$ satisfies the conditions of the theorem, and that $\kappa^{(1)}(\rho+)$ is finite. To prove the first part of the theorem suppose that the set $\{p_n^{(1)}(z)\}$ is effective in $|z| \leqq \rho$; then the known properties of $\kappa(r)$ [cf. 1; p. 449, Theorem 11.3] imply that $\kappa^{(1)}(\rho+) = \rho$ and (3.1) of Lemma 2 shows that $\kappa(R) = R$, so that the product set $\{p_n(z)\}$ is effective in $|z| \leqq R$.

To complete the proof of the theorem we first note that since $\kappa^{(1)}(\rho+)$ is finite and the set $\{p_n^{(2)}(z)\}$ is effective in $|z| \leqq R$, (3.1) implies that $\kappa(R+)$ is finite. Also Lemma 1 implies that the inverse set $\{{}^*p_n^{(2)}(z)\}$ is effective in $|z| \leqq \rho$, where ${}^*M^{(2)}(\rho)$ exists and is equal to R. Suppose now that the product set $\{p_n(z)\}$ is effective in $|z| \leqq R$. As we can put $\{p_n^{(1)}(z)\} = \{p_n(z)\}\{{}^*p_n^{(2)}(z)\}$, then the set $\{p_n(z)\}$, as an outer set, and $\{{}^*p_n^{(2)}(z)\}$, as an inner set, both satisfy the conditions of the "if"-statement of the theorem for $|z| = \rho$ and with $1/a$ for a. Consequently the product set $\{p_n^{(1)}(z)\}$ will be effective in $|z| \leqq \rho$ and the theorem is therefore established.

It should be observed that to prove the "if"-statement of the theorem the condition that $d_n^{(2)} = O(n)$ can be dispensed with. In fact, with the procedure of Lemma 2, the exclusion of the above condition leads to the "weaker" relation $\kappa(R) \leqq \lambda^{(2)}(R)\{\kappa^{(1)}(\rho+)/\rho\}^{\beta}$, from which the "if"-statment of the theorem can be deduced. This result has been given by Newns [cf. 1; p. 464, Theorem 22.1]. The fact that the other condition, ${}^*d_n^{(2)} = O(n)$, cannot be dropped is illustrated by the following example.

Example 3. Let m_k and c be defined as in Example 1, and consider the sets $\{p_n^{(1)}(z)\}$, $\{p_n^{(2)}(z)\}$ given by

$$p_n^{(1)}(z) = z^n, \quad (n \text{ even}); \quad p_n^{(1)}(z) = z^n - c^{(n+1)^2} z^{n+1}, \quad (n \text{ odd});$$

$$p_{m_k}^{(2)}(z) = z^{m_k}; \quad p_n^{(2)}(z) = z^n - z^{n+1}, \quad n \neq m_k; \quad k \geqq 0.$$

The set $\{p_n^{(1)}(z)\}$ is effective in $|z| \leqq r$ and $\kappa^{(1)}(r)$ is finite for $r > 0$. Also it is seen that the set $\{p_n^{(2)}(z)\}$ satisfies the conditions of the theorem for $0 < r \leqq 1$ and with $a = 1$, except that $\limsup_{n\to\infty} {}^*d_n^{(2)}/n = \infty$. The product set is easily seen to be not effective in $|z| \leqq 1$.

We finally append the following examples[3] to show that the theorem does not remain true if the condition $\kappa^{(1)}(aR+) < \infty$ is omitted or even weakened to $\kappa^{(1)}(aR+) = \kappa^{(1)}(aR-)$.

---

[3] These examples were suggested to me by the referee.

Example 4. Let $\{p_n(z)\}$ be the product of $\{p_n^{(1)}(z)\}$ and $\{p_n^{(2)}(z)\}$, where

$$p_n^{(1)}(z) = z^n \quad (n \text{ even}); \quad p_n^{(1)}(z) = z^n + z^{2n^2} \qquad (n \text{ odd});$$

$$p_0^{(2)}(z) = 1, \quad p_n^{(2)}(z) = n^{n\frac{1}{2}} + z^n \quad (n \text{ even} > 0); \quad p_n^{(2)}(z) = z^n \quad (n \text{ odd}).$$

The inner set is a simple set with leading coefficient unity, effective in $|z| \leqq r$ for all $r \geqq 1$. The outer set is effective in $|z| \leqq r$ for $r \leqq 1$, but $\kappa^{(1)}(1+) = \infty$. Now we find that

$$p_0(z) = 1, \; p_n(z) = n^{n\frac{1}{2}} + z^n \quad (n \text{ even} \geqq 0), \; p_n(z) = (2n^2)^{2\frac{1}{2}n} + z^n + z^{2n^2},$$

$(n \text{ odd})$, and that $\kappa(r) = \infty$ for all r.

Example 5. Consider now the product set $\{p_n^{(1)}(z)\} = \{p_n(z)\}\{{}^*p_n^{(2)}(z)\}$ where $\{p_n^{(1)}(z)\}$ and $\{p_n^{(2)}(z)\}$ are given in Example 4. The inner set satisfies the hypotheses of the theorem at $R = 1$ with $a = 1$. The outer set is no where effective, in fact $\kappa(1-) = \kappa(1+) = \infty$. However, the product set $\{p_n^{(1)}(z)\}$ is effective in $|z| \leqq 1$.

Finally, I should like to express my thanks to the referee of this note for the examples provided by him and for his other helpful and constructive suggestions.

ASSIUT UNIVERSITY,
ASSIUT, EGYPT.

REFERENCES.

[1] W. F. Newns, "On the representation of analytic functions by infinite series," *Philosophical Transactions of the Royal Society of London*, ser. A, vol. 245 (1953), pp. 429-468.

[2] M. N. Ghabbour, "On convergence of the product of basic sets of polynomials," *American Journal of Mathematics*, vol. 69 (1947), pp. 583-591.

A PROOF OF THE UNIQUENESS OF MINKOWSKI'S PROBLEM FOR CONVEX SURFACES.*

By Shiing-shen Chern.

For C'' closed convex surfaces in ordinary Euclidean space E the uniqueness of Minkowski's problem says that the knowledge of the Gaussian curvature (supposed to be strictly positive) as a function of the unit normal vector determines the surface up to a translation. Let S_0 be the unit sphere about the origin 0 in E. Since the normal map onto S_0 of a convex surface M with Gaussian curvature $K > 0$ is one-one, M can be defined by a vector-valued function $x(\xi)$, $\xi \in S_0$.

Let T be the space of all right-handed rectangular frames $0e_1e_2e_3$ about 0. Then T is a circle bundle over S_0, the projection being defined by mapping the frame into the end-point of the last vector e_3. Let $\theta_{ij} = -\theta_{ji} = de_ie_j$. (Throughout this note small Latin indices run from 1 to 3 and small Greek indices from 1 to 2.) Then we have

$$d\theta_{ij} = \sum_k \theta_{ik} \wedge \theta_{kj}. \tag{1}$$

On the other hand, let F be the space of all right-handed rectangular frames $xf_1f_2f_3$ in E ($\dim F = 6$). If we put

$$\omega_i = dx \cdot f_i, \qquad \omega_{ij} = -\omega_{ji} = df_if_j, \tag{2}$$

or

$$dx = \sum_i \omega_i f_i, \qquad df_i = \sum_j \omega_{ij} f_j, \tag{3}$$

we have

$$d\omega_i = \sum_j \omega_j \wedge \omega_{ji}, \qquad d\omega_{ij} = \sum_k \omega_{ik} \wedge \omega_{kj}. \tag{4}$$

The mapping $x\colon S_0 \to M$ defined by sending $\xi \in S_0$ into the point $x(\xi) \in M$ at which the unit normal vector is ξ induces a mapping $\tilde{x}\colon T \to F$, which sends the frame $0e_1e_2e_3$ to $x(e_3)e_1e_2e_3$. Let $\tilde{\omega}_i = \tilde{x}^*\omega_i$, $\tilde{\omega}_{ij} = \tilde{x}^*\omega_{ij}$ be the differential forms in T induced by $\tilde{x}$. Then we have $\tilde{\omega}_{ik} = \theta_{ik}$, $\tilde{\omega}_3 = 0$ and we can put

$$\tilde{\omega}_\alpha = \sum_\beta \lambda_{\alpha\beta}\theta_{\beta 3}, \qquad \lambda_{\alpha\beta} = \lambda_{\beta\alpha}. \tag{5}$$

where $\lambda_{11}\lambda_{22} - \lambda_{12}\lambda_{21} = 1/K(\xi)$.

* Received February 5, 1957.

Suppose there be a second convex surface M' defined by the vector-valued function $x'(\xi)$, with the same Gaussian curvature $K(\xi)$. We denote by dashes notions pertaining to M'. Then we have $\tilde{\omega}'_3 = \tilde{\omega}_3 = 0$, $\tilde{\omega}'_{ij} = \tilde{\omega}_{ij}$, and

$$\tilde{\omega}'_\alpha = \sum_\beta \lambda'_{\alpha\beta}\theta_{\beta 3}, \qquad \lambda'_{\alpha\beta} = \lambda'_{\beta\alpha}. \tag{6}$$

It suffices to prove that $\tilde{\omega}'_\alpha = \tilde{\omega}_\alpha$. For then $\tilde{x}'\tilde{x}^{-1}: \tilde{x}(T) \to \tilde{x}'(T)$ will be a one-one map under which $\omega'_i = (\tilde{x}'\tilde{x}^{-1})^*\omega_i$, $\omega'_{ij} = (\tilde{x}'\tilde{x}^{-1})^*\omega_{ij}$. By a well-known theorem on moving frames (E. Cartan, La théorie des groupes finis et continus . . . Paris, 1937), $\tilde{x}'\tilde{x}^{-1}$ is the identity, if it is the identity for one frame of $\tilde{x}(T)$. But this can be achieved by a translation.

To complete the proof we derive from (3), (5), (6) the formula

$$\begin{aligned} d(x, x', dx') &= p'(\tilde{\omega}_2 \wedge \tilde{\omega}'_1 - \tilde{\omega}_1 \wedge \tilde{\omega}'_2) + 2p\tilde{\omega}'_1 \wedge \tilde{\omega}'_2 \\ &= \{p' \begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} + \frac{2}{K}(p - p')\}\theta_{13} \wedge \theta_{23} \end{aligned}$$

where $p(\xi)$ is the distance from 0 to the tangent plane at $x(\xi)$. By Stokes Theorem we get

$$\int\int_{S_0} \{p' \begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} + \frac{2p}{K} - \frac{2p'}{K}\}\theta_{13} \wedge \theta_{23} = 0.$$

Since $(\lambda_{\alpha\beta})$ and $(\lambda'_{\alpha\beta})$ are positive definite symmetric matrices with the same determinant, it is well-known that

$$\begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} \leqq 0,$$

and that the equality sign holds only when $\lambda'_{\alpha\beta} = \lambda_{\alpha\beta}$. It follows that

$$\int\int_{S_0} \frac{1}{K}(p - p')\theta_{13} \wedge \theta_{23} \leqq 0$$

($p' < 0$, by choosing 0 to be in the interior of M'). But the relationship between M and M' is symmetrical, so that the relation still holds, when p and p' are interchanged. Hence the above integral is zero, and we have

$$\int\int_{S_0} p' \begin{vmatrix} \lambda'_{11} - \lambda_{11} & \lambda'_{12} - \lambda_{12} \\ \lambda'_{21} - \lambda_{21} & \lambda'_{22} - \lambda_{22} \end{vmatrix} \theta_{13} \wedge \theta_{23} = 0.$$

Here the integrand keeps a constant sign; the relation is possible, only when the integrand vanishes identically, which in turn implies $\lambda'_{\alpha\beta} = \lambda_{\alpha\beta}$. This completes our proof.

UNIVERSITY OF CHICAGO.

CORRESPONDENCE.*

A correspondent, who wishes to remain anonymous, writes as follows:

. . . Una notissima congettura di F. Severi (*Rend. Pal.* 28 (1909), p. 45) asserisce che "*ogni varietà dotata di punti multipli si può considerare come limite di una senza singolarità, appartenente allo stesso spazio.*"

Secondo una notizia orora diffusa da Nancago dall'agenzia "United Press," l'ipotesi dell'illustre autore sarebbe stata confutata dall'egregio geometra francese Renato Thom, basandosi sull'esempio dei coni del 3° ordine nello spazio S_6 e mediante assai delicate considerazioni topologiche.

Forse non dispiacerà ai lettori del Suo pregiato periodico trovare qui una trattazione geometrica elementare dell'esempio di Thom. Di fatti, si determineranno tutte le varietà del 3° ordine in uno spazio S_n qualunque. Questo trarrà con sè, come conseguenza immediata, la falsità dell'ipotesi suddetta.

Sia V_r una varietà del 3° ordine nello spazio S_n, di dimensione $r < n-1$, non contenuta in un iperpiano. Sia C il cono, proiettante la V_r da un punto semplice qualunque M di V_r; sia M' un altro punto di V_r, semplice sul cono C. Il cono C è del secondo ordine; quindi la sua proiezione da M' è una varietà lineare di dimensione $r+1$, sicché la V_r è contenuta in una varietà lineare di dimensione $r+2$. È dunque $r = n-2$, e C hà la dimensione $n-1$. Lo stesso vale per il cono C', proiettante V_r da M'. I coni C, C' sono distinti, giacché M' è semplice sul cono C; la loro intersezione è dunque una varietà riducibile del 4° ordine, spezzata nella V_r e una varietà lineare. Siano $A = 0$, $B = 0$ le equazioni di quest'ultima. Allora si possono scrivere le equazioni dei coni C, C' nella forma:

$$(1) \qquad AP = BQ, \qquad AP' = BQ',$$

denotando con P, Q, P', Q' quattro forme lineari nelle coordinate omogenee nello spazio. Sia s il numero di forme indipendenti fra le sei forme A, B, P, Q, P', Q'; questo è almeno 4, giacché, se fosse 2, i coni C, C' non sarebbero irriducibili, e, se fosse 3, la loro intersezione si spezzerebbe in quattro varietà lineari distinte o coincidenti. I valori possibili per s sono quindi 4, 5 e 6.

* Received June 3, 1957.

Sia L la varietà lineare, di dimensione $n-s$, definita dalle equazioni $A=B=0$, $P=Q=P'=Q'=0$. Ogni varietà lineare, proiettante da L un punto dell'intersezione di C e C', è contenuta in questa, come si vede subito sulle equazioni (1). Proiettando V_r da L, si ottiene quindi una varietà W del 3° ordine di dimensione $s-3$ in uno spazio S_{s-1}; e V_r non è altro che il cono proiettante W da L. Nello spazio S_{s-1}, si può prendere per coordinate omogenee s forme indipendenti fra le forme A, B, P, Q, P', Q'; allora le equazioni (1) vi definiscono una varietà del 4° ordine, spezzata nella W e una varietà lineare. Adesso distinguiamo tre casi:

(a) $s=6$: W è la varietà di Segre W_3 immersa in S_5, immagine birazionale senza eccezione del prodotto di un piano e una retta; come è noto, è priva di punti multipli.

(b) $s=5$: W è sezione iperpiana della sopradetta W_3. È facile vedere che tutte le sezioni iperpiane irriducibili della W_3 sono proiettivamente equivalenti fra di loro; denotando con W_2 una di esse, è anch'essa una varietà razionale senza punti multipli.

(c) $s=4$: W è la ben nota cubica razionale W_1 immersa in S_3.

Così è dimostrato che ogni varietà del 3° ordine appartiene a uno dei seguenti tipi:

1° le varietà di dimensione r, contenute in una varietà lineare di dimensione $r+1$;

2° le tre varietà razionali W_3, W_2, W_1 enumerate disopra;

3° i coni proiettanti una di queste tre da una varietà lineare di dimensione qualunque.

Evidentemente, una varietà del secondo o terzo tipo non può essere limite di una varietà del primo tipo, e perciò una varietà del terzo tipo, di dimensione maggiore di 3, non può essere limite di varietà prive di punti multipli.

X. X. X.

ni
L
le
na
è
er
V';
ta

i-
o,

re
te
tà

ei

di

n-

re
o,
ti

du
in

fo
m

ne

av

fo
m

(

ti
sy

m
su
ca

sy
a
a
is
L

li

si
B
p
st

th
th

c
b

(
a

f
[

I

‘
a
b

c
c

ON THE PREPARATION OF MANUSCRIPTS.

The following instructions are suggested or dictated by the necessities of the technical production of the American Journal of Mathematics. Authors are urged to comply with these instructions, which have been prepared in their interests.

Manuscripts not complying with the standards usually have to be returned to the authors for typographic explanation or revisions and the resulting delay often necessitates the deferment of the publication of the paper to a later issue of the Journal.

Horizontal fraction signs should be avoided. Instead of them use either solidus signs / or negative exponents.

Neither a solidus nor a negative exponent is needed in the symbols $\frac{1}{2}$, $\frac{1}{\pi}$, $\frac{1}{2\pi}$, $\frac{1}{2\pi i}$, which are available in regular size type.

Binomial coefficients should be denoted by C_k^n and not by parentheses. Correspondingly, for symbols of the type of a quadratic residue character the use of some non-vertical arrangement is usually imperative.

Use the exponent $\frac{1}{2}$ instead of the square root sign.

Replace $e^{(\ )}$ by exp( ) if the expression in the parenthesis is complicated.

By an appropriate choice of notations, avoid unnecessary displays.

Simple formulae, such as $A + iB = \frac{1}{2}C^*$ or $s_n = a_1 + \cdots + a_n$, should not be displayed (unless they need a formula number).

Use $'$ or $d\ /dx$, possibly D, but preferably not a dot, in order to denote ordinary differentiation and, as far as possible, a subscript in order to denote partial differentiation (when the symbol ∂ cannot be avoided, it should be used as $\partial\ /\partial x$).

Commas between indices are usually superfluous and should be avoided if possible.

In a determinant use a notation which reduces it to the form det a_{ik}.

Subscripts and superscripts cannot be printed in the same vertical column, hence the manuscript should be clear on whether $a_i{}^k$ or $a^k{}_i$ is preferred. (Correspondingly, the limits of summation must not be typed *after* the Σ-sign, unless either $\Sigma_1{}^m$ or $\Sigma^m{}_1$ is desired.) If a letter carrying a subscript has a prime, indicate whether $x_i{}'$ or $x'{}_i$ is desired.

Experience shows that a tilde or anything else *over* a letter is very unsatisfactory. Such symbols often drop out of the type after proof-reading and, when they do not, they usually appear uneven in print. For these reasons we advise against their use. This advice applies also to a bar over a Greek or German letter (for the symbol of complex conjugation an asterisk is often allowed by the context). Type carrying bars over ordinary size italic letters of the Latin alphabet is available.

Bars reaching over several letters should in any case be avoided (in particular, type lim sup and lim inf instead of lim with upper and lower bars).

Repeated subscripts and superscripts should be used only when they cannot be avoided, since the index of the principal index usually appears about as large as the principal index. Bars and other devices *over* indices cannot be supplied. On the other hand, an asterisk or a prime (to be printed *after* the subscript) is possible on a subscript. The same holds true for superscripts.

Distinguish carefully between l. c. "oh," cap. "oh" and zero. One way of distinguishing them is by underlining one or two of them in different colors and explaining the meaning of the colors.

Distinguish between ϵ (epsilon) and $\in$ or ε (symbol), between x (eks) and $\times$ (multiplication sign), between l. c. and cap. phi, between l. c. and cap. psi, between l. c. k and kappa and between "ell" and "one" (for the latter, use l and 1 respectively).

Avoid unnecessary footnotes. For instance, references can be incorporated into the text (parenthetically, when necessary) by quoting the number in the bibliographic list, which appear at the end of the paper. Thus: "[3], pp. 261-266."

Except when informality in referring to papers or books is called for by the context, the following form is preferred:

[3] O. K. Blank, "Zur Theorie des Untermengenraumes der abstrakten Leermenge," *Bulletin de la Societé Philharmonique de Zanzibar*, vol. 26 (1891), pp. 242-270.

In any case, the references should be precise, unambiguous and intelligible.

Usually sections numbers and section titles are printed in bold face, the titles "Theorem," "Lemma" and "Corollary" are in caps and small caps, "Proof," "Remark" and "Definition" are in italics. This (or a corresponding preference) should be marked in the manuscript. Use a period, and *not* a colon, after the titles Theorem, Lemma, etc.

German, script and bold face letters should be underlined in various colors and the meaning of the colors should be explained. The same device is needed for Greek letters if there is a chance of ambiguity. In general, mark all cap. Greek letters.

All instructions and explanations for the printer can conveniently be collected on a separate sheet, to be attached to the manuscript.

In case of doubt, recent issues of the Journal may be consulted.

m